REFERENCE GUIDE

Cisco Small Business Pro

SPS208G/SPS224G4/SPS2024 Ethernet Switches Command Line Interface

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Introduction

Overview

This document describes the Command Line Interface (CLI) used to manage the Linksys SPS208G, SPS224G4, and SPS2024 switches. Unless noted otherwise, all of the CLI commands in this document apply to all three switches.

This chapter describes the CLI command modes, how to access the CLI, and the CLI command editing features.

CLI Command Modes

For greater ease of use, the Command Line Interface (CLI) is divided into four command modes arranged hierarchically by privilege level. The command modes are (in the order in which they are accessed):

- User EXEC mode (lowest privilege)
- Privileged EXEC mode
- Global Configuration mode
- Interface Configuration mode (highest privilege)

Each command mode has its own unique console prompt and set of CLI commands. Entering a question mark at the console prompt displays a list of available commands for the current mode. Specific commands are used to switch from one mode to another.

User EXEC Mode

This is the initial mode after system login (except for users who are defined as privileged users; refer to "*Privileged EXEC Mode*"). User EXEC mode is used for tasks that do not change the configuration, such as performing basic tests and listing system information.

The user-level prompt consists of the Switch host name followed by the angle bracket >:

```
Console>
```

The default host name is **Console** unless it is changed via the **hostname** command in Global Configuration mode.

To access the next higher mode (Privileged EXEC mode), use the **enable** command and enter a password when prompted.

Privileged EXEC Mode

Privileged EXEC mode is password-protected to prevent unauthorized use, as many of its commands set operating system parameters. The password is not displayed on the screen and is case-sensitive.

Privileged users start in Privileged EXEC mode. To enter this mode from User EXEC mode, follow these steps:

STEP 1 At the prompt enter the **enable** command and press **Enter**. A password prompt is displayed.

STEP 2 Enter the password and press **Enter**. (For security purposes, each character in the password is replaced by *). The Privileged EXEC mode prompt, consisting of the Switch host name followed by, is displayed.

```
Console#
```

To return from the Privileged EXEC mode to the User EXEC mode, use the **disable** command.

The following example illustrates how to access Privileged EXEC mode and then return to User EXEC mode:

```
Console> enable

Enter Password: ******
```

```
Console#

Console# disable

Console>
```

Global Configuration Mode

The Global Configuration mode is used to configure features at the system level, and not at the interface level.

To access Global Configuration mode from Privileged EXEC mode, enter the **configure** command at the Privileged EXEC mode prompt and press **Enter.** The Global Configuration mode prompt, consisting of the device host name followed by **(config)#**, is displayed:

```
Console(config)#
```

Use any of the following commands to return from Global Configuration mode to the Privileged EXEC mode:

```
exit

end

Ctrl+Z
```

The following example shows how to access Global Configuration mode and return to Privileged EXEC mode:

```
Console#

Console# configure

Console(config)# exit

Console#
```

Interface Configuration Mode

Interface Configuration mode commands perform operations on specific interfaces. This mode is divided into the following submodes, each with a specific function:

- Line Interface — Contains commands used to configure the management connections. These include commands such as line timeout settings, etc. The **line** Global Configuration mode command is used to enter the Line Configuration command mode.
- VLAN Database — Contains commands used to create a VLAN as a whole. The **vlan database** Global Configuration mode command is used to enter the VLAN Database Interface Configuration mode.
- Management Access List — Contains commands used to define management access-lists. The **management access-list** Global Configuration mode command is used to enter the Management Access List Configuration mode.
- Ethernet — Contains commands used to manage port configuration. The **interface ethernet** Global Configuration mode command is used to enter the Interface Configuration mode.
- Port Channel — Contains commands used to configure port-channels; for example, assigning ports to a port-channel. Most of these commands are the same as the commands in the Ethernet interface mode, and are used to manage the member ports as a single entity. The **interface port-channel** Global Configuration mode command is used to enter the Port Channel Interface Configuration mode.
- SSH Public Key-chain — Contains commands used to manually specify other device SSH public keys. The **crypto key pubkey-chain ssh** Global Configuration mode command is used to enter the SSH Public Key-chain Configuration mode.
- QoS — Contains commands related to service definitions. The **qos** Global Configuration mode command is used to enter the QoS services configuration mode.
- MAC Access-List — Configures conditions required to allow traffic based on MAC addresses. The **mac access-list** Global Configuration mode command is used to enter the MAC access-list configuration mode.

To return from any Interface Configuration mode to the Global Configuration mode, use the **exit** command.

Accessing the Command Line Interface

The Command Line Interface (CLI) can be accessed from a terminal or computer by performing one of the following tasks:

- Running a terminal application, such as HyperTerminal, on a computer that is directly connected to the Switch's console port,

  —or—

- Running a telnet session from a command prompt on a computer with a network connection to the Switch.

If access is via a telnet connection, ensure that the following conditions are met before using CLI commands:

- The Switch has a defined IP address.
- Corresponding management access is granted.
- The workstation used to access the Switch is connected to the Switch.

Using HyperTerminal over the Console Interface

NOTE When using HyperTerminal with Microsoft® Windows® 2000, ensure that Windows® 2000 Service Pack 2 or later is installed on your computer. The arrow keys will not function properly using HyperTerminal's VT100 emulation in Windows® 2000 prior to Service Pack 2. For information on Windows® 2000 service packs, go to www.microsoft.com.

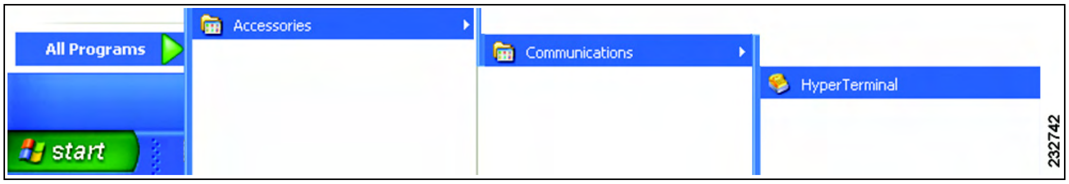
The Switch's RS-232 serial console port provides a direct connection to a computer's serial port using a standard DB-9 null-modem or crossover cable. Once the computer and Switch are connected, run a terminal application such as HyperTerminal to access the Command Line Interface.

To access the Command Line Interface using the HyperTerminal application, perform the following steps:

STEP 1 Click the **Start** button.

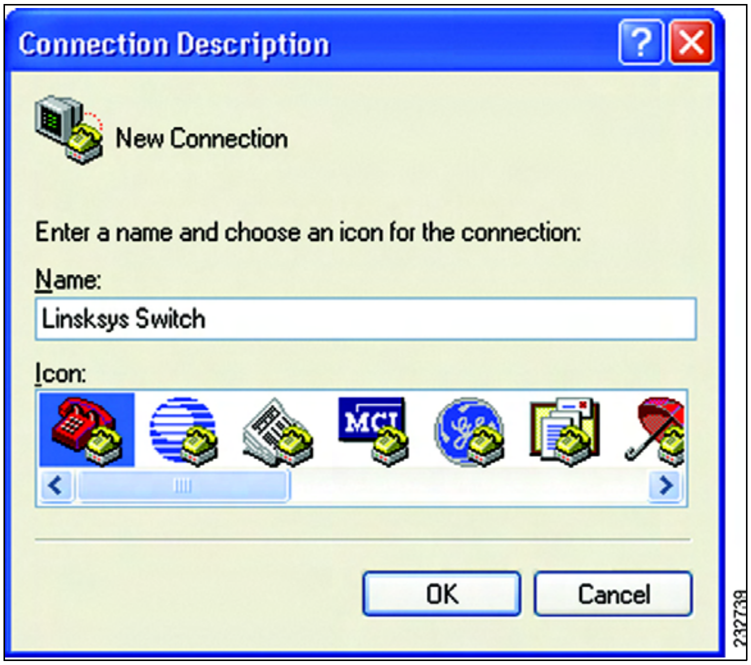
STEP 2 Select **All Programs** > **Accessories** > **Communications** > **HyperTerminal.**

Figure 1 Start > All Programs > Accessories > Communications > HyperTerminal



STEP 3 Enter a name for this connection. Select an icon for the application, then click **OK**.

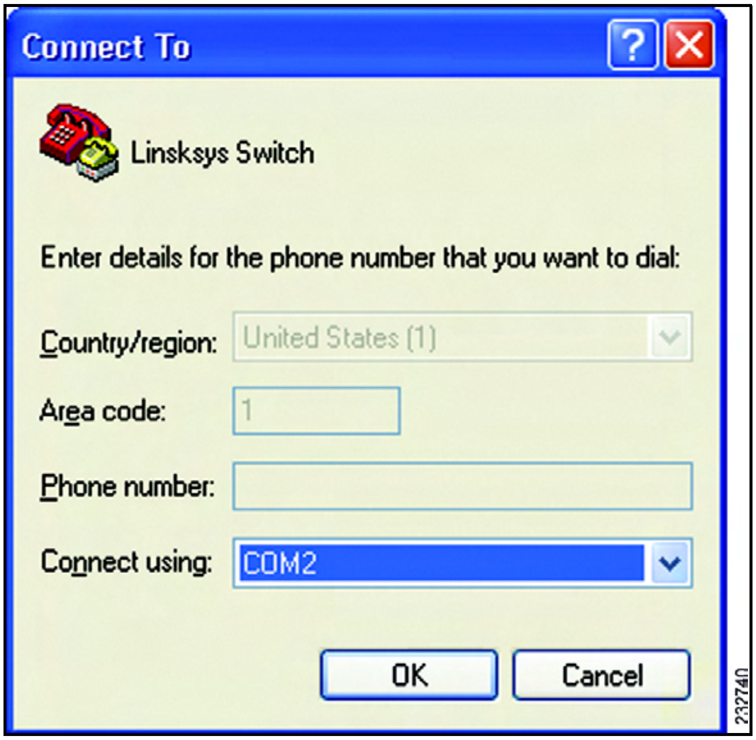
Figure 2 HyperTerminal Connection Description Screen



Linsksys Switch

STEP 4 Select a port to communicate with the switch. Select **COM1** or **COM2**.

Figure 3 HyperTerminal Connect To Screen



Connect To

Linsksys Switch

Enter details for the phone number that you want to dial:

Country/region: United States (1)

Area code: 1

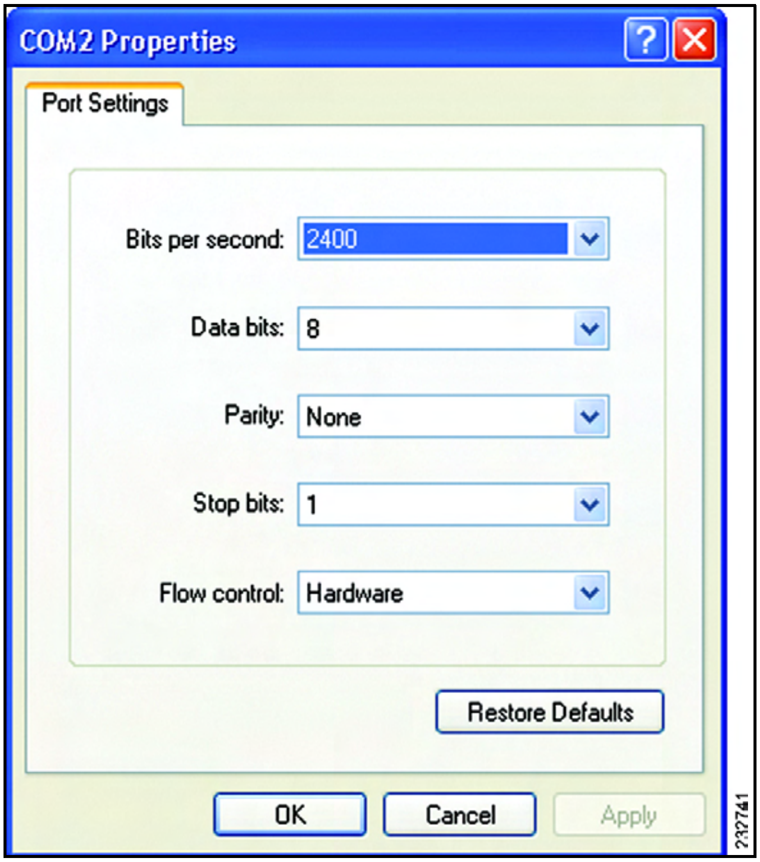
Phone number:

Connect using: COM2

STEP 5 Set the serial port settings as follows, then click **OK**.

- Bits per Second: **38400**
- Databits: **8**
- Parity: **one**
- Stop bits: **1**
- Flow control: **None**

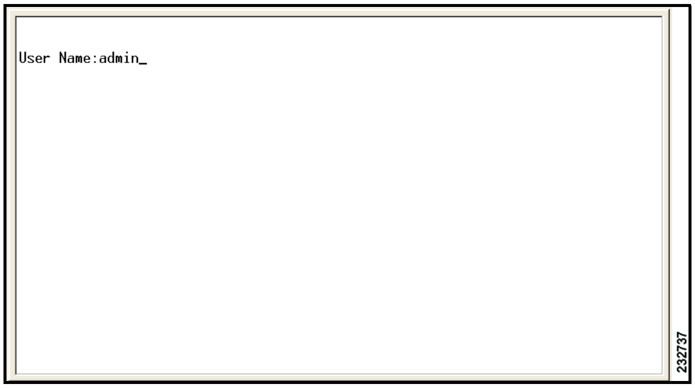
Figure 4 HyperTerminal Properties Screen



Bits per second: 2400
Data bits: 8
Parity: None
Stop bits: 1
Flow control: Hardware

STEP 6 When the *Command Line Interface* appears, enter **admin** at the *User Name* prompt and press **Enter**.

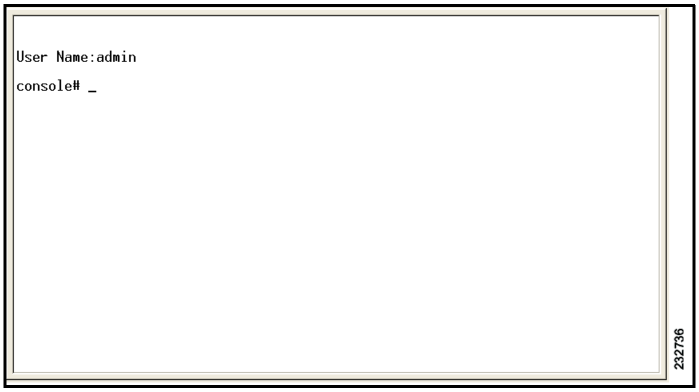
Figure 5 Command Line User Name Prompt



```
User Name:admin_
```

The **console#** prompt is displayed. This prompt is where you enter CLI commands.

Figure 6 Command Line



```
User Name:admin
console# _
```

You can now enter CLI commands to manage the Switch. For detailed information on CLI commands, refer to the appropriate chapter(s) of this Reference Guide.

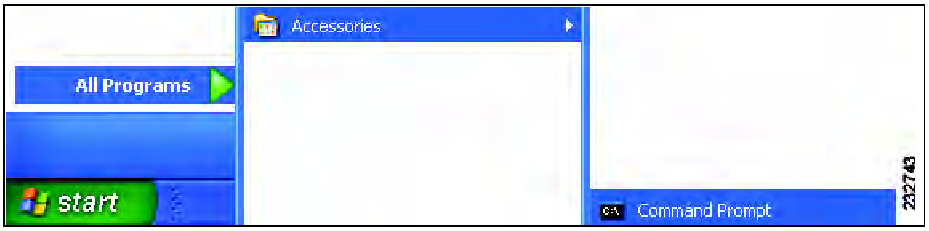
Using Telnet over an Ethernet Interface

Telnet provides a method of connecting to the Command Line Interface using TCP/IP over a standard Ethernet connection. A telnet session can be established in HyperTerminal or from a command prompt.

To establish a telnet session from the command prompt, perform the following steps:

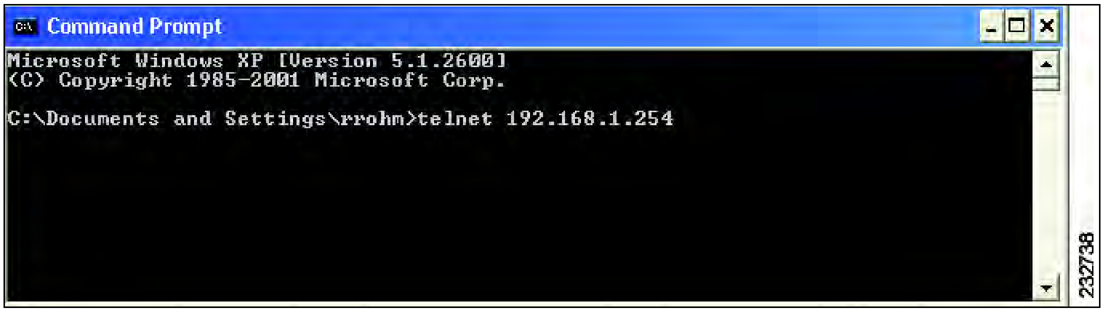
STEP 1 Click **Start**, then select **All Programs** > **Accessories** > **Command Prompt** to open a command prompt.

Figure 7 Start > All Programs > Accessories > Command Prompt



STEP 2 At the prompt, enter **telnet 192.168.1.254**, then press **Enter**.

Figure 8 Command Prompt

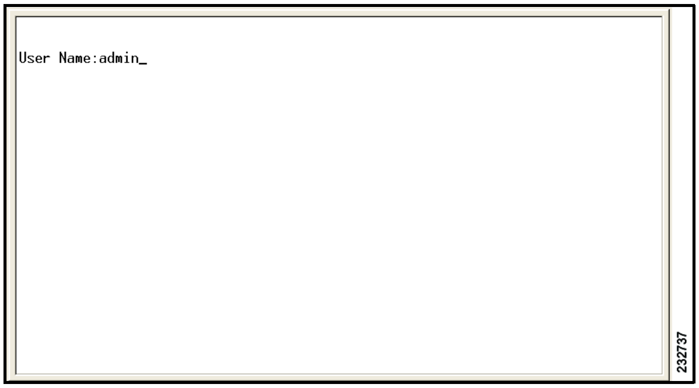


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\rrohm>telnet 192.168.1.254
```

STEP 3 The *Command Line Interface* will be displayed. Enter **admin** at the *User Name* prompt and press **Enter**.

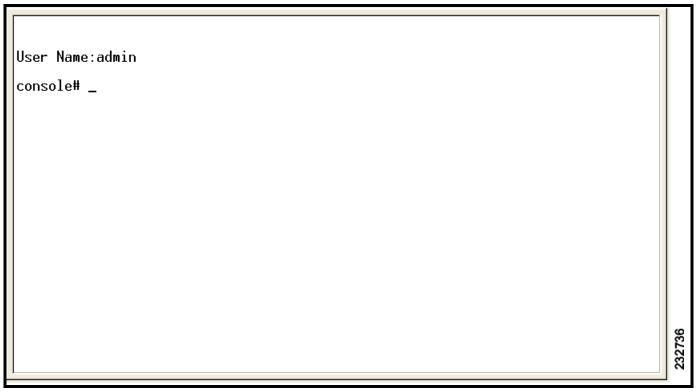
Figure 9 Command Line User Name Prompt



```
User Name:admin_
```

STEP 4 The **console#** prompt is displayed. This prompt is where you enter CLI commands.

Figure 10 Command Line



```
User Name:admin
console# _
```

You can now enter CLI commands to manage the Switch. For detailed information on CLI commands, refer to the appropriate chapter(s) of this Reference Guide.

Editing Features

Entering Commands

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command **show interfaces status ethernet e11**, *show*, *interfaces* and *status* are keywords, *ethernet* is an argument that specifies the interface type, and *e11* specifies the port.

To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)# username admin password alansmith
```

When working with the CLI, the command options are not displayed. The command is not selected from a menu, but is manually entered. To see what commands are available in each mode or within an Interface Configuration, the CLI does provide a method of displaying the available commands, the command syntax requirements and in some instances parameters required to complete the command. The standard command to request help is ?.

There are two instances where help information can be displayed:

- Keyword lookup — The character **?** is entered in place of a command. A list of all valid commands and corresponding help messages are is displayed.
- Partial keyword lookup — If a command is incomplete and or the character **?** is entered in place of a parameter, the matched keyword or parameters for this command are displayed.

To assist in using the CLI, there is an assortment of editing features. The following features are described:

- Terminal Command Buffer
- Command Completion
- Nomenclature
- Keyboard Shortcuts

Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a First In First Out (FIFO) basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets.

Keyword	Description
Up-Arrow key Ctrl+P	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-Arrow key	Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence will recall successively more recent commands.

By default, the history buffer system is enabled, but it can be disabled at any time. For more information on enabling or disabling the history buffer, refer to the **history** command.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 216. By configuring 0, the effect is the same as disabling the history buffer system. For more information on configuring the command history buffer, refer to the **history size** command.

To display the history buffer, refer to the **show history** command.

Negating the Effect of Commands

For many configuration commands, the prefix keyword **no** can be entered to cancel the effect of a command or reset the configuration to the default value. This Reference Guide provides a description of the negation effect for each CLI command.

Command Completion

If the command entered is incomplete, invalid or has missing or invalid parameters, then the appropriate error message is displayed. This assists in entering the correct command. By pressing **Tab** after an incomplete command is entered, the system will attempt to identify and complete the command. If the characters already entered are not enough for the system to identify a single matching command, press **?** to display the available commands matching the characters already entered.

Nomenclature

Within the CLI, Ethernet ports are denoted as follows:

Switch	10/100 Ethernet ports	Gigabit Ethernet ports
SPS208G	e1 through e8	g1 through g2
SPS224G4	e1 through e24	g1 through g4
SPS2024	n/a	g1 through g24

The ports may be described on an individual basis or within a range. Use format port number-port number to specify a set of consecutive ports and port number, port number to indicate a set of non-consecutive ports. For example, **g1-3** stands for Gigabit Ethernet ports 1, 2, and 3, and **g1,5** stands for Gigabit Ethernet ports 1 and 5.

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The following table describes the CLI shortcuts.

Keyboard Key	Description
Up-arrow	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow	Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any configuration mode.
Backspace	Deletes one character left to the cursor position.

CLI Command Conventions

When entering commands there are certain command entry standards that apply to all commands. The following table describes the command conventions.

Convention	Description
[ ]	In a command line, square brackets indicate an option entry.
{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated the | character. One option must be selected. For example, **flowcontrol {auto|on|off}** means that for the flowcontrol command, either auto, on, or off must be selected.
parameter	Italic text indicates a parameter.

Convention	Description
press **key**	Names of keys to be pressed are shown in **bold.**
Ctrl+F4	Keys separated by the + character are to be pressed simultaneously on the keyboard
Screen Display	Fixed-width font indicates CLI prompts, CLI commands entered by the user, and system messages displayed on the console.
all	When a parameter is required to define a range of ports or parameters and all is an option, the default for the command is all when no parameters are defined. For example, the command interface range port-channel has the option of either entering a range of channels, or selecting all. When the command is entered without a parameter, it automatically defaults to all.

Copying and Pasting Text

Up to 1000 lines of text (or commands) can be copied and pasted into the device.

NOTE It is the user's responsibility to ensure that the text copied into the device consists of legal commands only.

This feature is dependent on the baud rate of the device.

When copying and pasting commands from a configuration file, make sure that the following conditions exist:

- A device Configuration mode has been accessed.
- The commands contain no encrypted data, like encrypted passwords or keys. Encrypted data cannot be copied and pasted into the device.

2

AAA Commands

aaa authentication login

The **aaa authentication login** Global Configuration mode command defines login authentication. To restore defaults, use the no form of this command.

Syntax

aaa authentication login {default | *list-name*} *method1* [*method2...*]

no aaa authentication login {**default** | *list-name*}

Parameters

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
- *list-name* — Character string used to name the list of authentication methods activated when a user logs in. (Range: 1-12 characters)
- *method1* [*method2...*] — Specify at least one method from the following list:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.

Keyword	Description
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the command aaa authentication login *list-name local.*

NOTE If the authentication method is not defined, console users will be able to log in without any authentication check.

Command Mode

Global Configuration mode

User Guidelines

The default and optional list names created with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** *list-name method* command for a particular protocol, where *list-name* is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line.

Example

The following example configures the authentication login:

```
Console(config)# aaa authentication login default radius tacacs
enable line local none
```

aaa authentication enable

The **aaa authentication enable** Global Configuration mode command defines authentication method lists for accessing higher privilege levels. To restore defaults, use the **no** form of this command.

Syntax

aaa authentication enable {default | *list-name*} *method1* [*method2...*]

no aaa authentication enable default

Parameters

- **default** — Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
- *list-name* — Character string used to name the list of authentication methods activated, when using access higher privilege levels. (Range: 1-12 characters)
- *method1* [*method2...*] — Specify at least one method from the following list:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

If the **default** list is not set, only the enable password is checked. This has the same effect as the command **aaa authentication enable default enable.**

On the console, the enable password is used if it exists. If no password is set, the process still succeeds. This has the same effect as using the command **aaa authentication enable default enable none**.

Command Mode

Global Configuration mode

User Guidelines

The default and optional list names created with the **aaa authentication enable** command are used with the **enable authentication** command.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

All **aaa authentication enable** *default* requests sent by the device to a RADIUS or TACACS+ server include the username $enabx$., where x is the requested privilege level.

Example

The following example sets the enable password for authentication when accessing higher privilege levels.

```
Console(config)# aaa authentication enable default enable
```

login authentication

The **login authentication** Line Configuration mode command specifies the login authentication method list for a remote telnet or console. To restore the default configuration specified by the **aaa authentication login** command, use the **no** form of this command.

Syntax

login authentication {default | *list-name*}

no login authentication

Parameters

- **default —** Uses the default list created with the **aaa authentication login** command.
- *list-name* —Uses the indicated list created with the **aaa authentication login** command.

Default Configuration

Uses the default set with the command **aaa authentication login.**

Command Mode

Line Configuration mode

User Guidelines

To change (or rename) an authentication method, use the negate command and create a new rule with the new method name.

Example

The following example specifies the default authentication method for a console.

```
Console(config)# line console
Console(config-line)# login authentication default
```

enable authentication

The **enable authentication** Line Configuration mode command specifies the authentication method list when accessing a higher privilege level from a remote Telnet or console. To restore the default configuration specified by the **aaa authentication enable** command, use the **no** form of this command.

Syntax

enable authentication {default | *list-name*}

no enable authentication

Parameters

- **default —** Uses the default list created with the **aaa authentication enable** command.
- *list-name* — Uses the indicated list created with the **aaa authentication enable** command.

Default Configuration

Uses the default set with the **aaa authentication enable** command.

Command Mode

Line Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the default authentication method when accessing a higher privilege level from a console.

```
Console(config)# line console
Console(config-line)# enable authentication default
```

ip http authentication

The **ip http authentication** Global Configuration mode command specifies authentication methods for HTTP server users. To restore the default configuration, use the **no** form of this command.

Syntax

ip http authentication *method1* [*method2...*]

no ip http authentication

Parameters

- *method1* [*method2...*] — Specify at least one method from the following list:

Keyword	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the command **ip http authentication** *local*.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Example

The following example configures the HTTP authentication.

```
Console(config)# ip http authentication radius tacacs local none
```

ip https authentication

The **ip https authentication** Global Configuration mode command specifies authentication methods for HTTPS server users. To restore the default configuration, use the **no** form of this command.

Syntax

ip https authentication *method1* [*method2...*]

no ip https authentication

Parameters

- *method1* [*method2...*] — Specify at least one method from the following list:

Keyword	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is checked. This has the same effect as the command **ip https authentication** *local*.

Command Mode

Global Configuration mode

User Guidelines

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

Example

The following example configures HTTPS authentication.

```
Console(config)# ip https authentication radius tacacs local
none
```

show authentication methods

The **show authentication methods** Privileged EXEC mode command displays information about the authentication methods.

Syntax

show authentication methods

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the authentication configuration.

```
Console# show authentication methods

Login Authentication Method Lists
---------------------------------
Default: Radius, Local, Line


Enable Authentication Method Lists
----------------------------------
Default: Radius, Enable
Console_Enable: Enable, None


LineLogin Method ListEnable Method List
-----------------------------------------------
ConsoleConsole_LoginConsole_Login
TelnetDefaultDefault
SSHDefaultDefault

http: Radius, Local
https: Radius, Local
dot1x: Radius
```

password

The **password** Line Configuration mode command specifies a password on a line. To remove the password, use the **no** form of this command.

Syntax

password *password* [**encrypted**]

no password

Parameters

- *password* — Password for this level. (Range: 1-159 characters)
- **encrypted** — Encrypted password to be entered, copied from another device configuration.

Default Configuration

No password is defined.

Command Mode

Line Configuration mode

User Guidelines

If a password is defined as encrypted, the required password length is 32 characters.

Example

The following example specifies the password called ‘secret’ on a console.

```
Console(config)# line console
Console(config-line)# password secret
```

enable password

The **enable password** Global Configuration mode command sets a local password to control access to user and privilege levels. To remove the password requirement, use the **no** form of this command.

Syntax

enable password [level *level*] *password* **encrypted]**

no enable password [level *level]*

Parameters

- *password* — Password for this level. (Range: 1-159 characters)
- *level* — Level for which the password applies. If not specified the level is 15 (Range: 1-15).
- **encrypted —** Encrypted password entered, copied from another device configuration.

Default Configuration

No enable password is defined.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets a local level 15 password called ‘secret’ to control access to user and privilege levels.

```
Console(config)# enable password secret level 15
```

username

The **username** Global Configuration mode command creates a user account in the local database. To remove a user name, use the **no** form of this command.

Syntax

username *name* [**password** *password*] [**level** *level*] [**encrypted**]

no username *name*

Parameters

- *name* — The name of the user. (Range: 1-20 characters)
- *password* — The authentication password for the user. (Range: 1-159 characters)
- *level* — The user level (Range: 1-15). If a level is not specified, the level is automatically set to 1.
- **encrypted** — Encrypted password entered, copied from another device configuration.

Default Configuration

No user is defined.

Command Mode

Global Configuration mode

User Guidelines

User account can be created without a password.

Example

The following example configures a user named ‘bob’ with password ‘lee’ and user level 15 to the system.

```
Console(config)# username bob password lee level 15
```

show users accounts

The **show users accounts** Privileged EXEC mode command displays information about the users local database.

Syntax

show users accounts

Default Configuration

No default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

User account can be created without a password.

Example

The following example displays information about the users local database.

```
Console# show users accounts
```

```
Username      Privilege
--------      ---------
Bob           15
Robert        15
Smith         15
```

show privilege

To display your current level of privilege, use the show privilege command in EXEC mode.

Syntax

show privilege

Parameters

This command has no arguments or key words

Default Configuration

This command has no default configuration.

Command Mode

EXEC

Example

```
Console# show privilege

Current privilege level is 15
```

ACL Commands

ip access-list

The **ip access-list** Global Configuration mode command enables the IP-Access Configuration mode and creates Layer 3 ACLs. To delete an ACL, use the **no** form of this command.

Syntax

ip access-list *access-list-name*

```
no ip access-list access-list-name
```

Parameters

- *access-list-name* — Specifies the name of the ACL. (Range: 0-32 characters) Use “” for empty string.

Default Configuration

The default for all ACLs is **deny-all**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to create an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-al)#
```

permit (ip)

The **permit** IP-Access List Configuration mode command permits traffic if the conditions defined in the permit statement match.

Syntax

permit {**any** | *protocol*} {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} [**dscp** *dscp-number* | **ip-precedence** *ip-precedence*]

permit-icmp {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} {**ny** | *icmp-type*} {**any** | *icmp-code*} [**dscp** *dscp-number* | **ip-precedence** *ip-precedence*]

permit-igmp {**any** | {*source source-wildcard*}} {**any** | {*destination destination-wildcard*}} {**ny** | *igmp-type*} [**dscp** *dscp-number* | **ip-precedence** *ip-precedence*]

permit-tcp {**any** | {*source source-wildcard*}} {**any** | *source-port*} {**any** |{*destination destination-wildcard*}} {**ny** |*destination-port*} [**dscp** *dscp-number*| **ip-precedence** *ip-precedence*] [**flags** *list-of-flags*]

permit-udp {**any** | {*source source-wildcard*}} {**any** | *source-port*} {**any** | {*destination destination-wildcard*}} {**any** | *destination-port*} [**dscp** *dscp-number* | **ip-precedence** *ip-precedence*]

Parameters

- *source* — Specifies the source IP address of the packet. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *source-wildcard* — Specifies wildcard to be applied to the source IP address. Use 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.

- *destination* — Specifies the destination IP address of the packet. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination-wildcard* — Specifies wildcard to be applied to the destination IP address. Use 1s in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *protocol* — Specifies the abbreviated name or number of an IP protocol. (Range: 0-255). The following table lists the protocols that can be specified:

IP Protocol	Abbreviated Name	Protocol Number
Internet Control Message Protocol	icmp	1
Internet Group Management Protocol	igmp	2
IP in IP (encapsulation) Protocol	ip	4
Transmission Control Protocol	tcp	6
Exterior Gateway Protocol	egp	8
Interior Gateway Protocol	igp	9
User Datagram Protocol	udp	17
Host Monitoring Protocol	hmp	20
Reliable Data Protocol	rdp	27
Inter-Domain Policy Routing Protocol	idpr	35
Ipv6 protocol	ipv6	41
Routing Header for IPv6	ipv6-route	43
Fragment Header for IPv6	ipv6-frag	44
Inter-Domain Routing Protocol	idrp	45
Reservation Protocol	rsvp	46
General Routing Encapsulation	gre	47
Encapsulating Security Payload (50)	esp	50
Authentication Header	ah	51
ICMP for IPv6	ipv6-icmp	58

IP Protocol	Abbreviated Name	Protocol Number
(any IP protocol)	any	(25504)
EIGRP routing protocol	eigrp	88
Open Shortest Path Protocol	ospf	89
IP-within-IP Encapsulation Protocol	ipip	94
Protocol Independent Multicast	pim	103
Layer Two Tunneling Protocol	l2tp	115
ISIS over IPv4	isis	124

- **dscp** — Indicates matching the *dscp-number* with the packet dscp value. (Range: 0-63)
- **ip-precedence** — Indicates matching the *ip-precedence* number with the packet ip-precedence value. (Range: 0-7)
- *icmp-type* — Specifies an ICMP message type for filtering ICMP packets. Enter a value or one of the following values: **echo-reply**, **destination-unreachable**, **source-quench**, **redirect**, **alternate-host-address**, **echorequest**, **router-advertisement**, **router-solicitation**, **time-exceeded**, **parameter-problem**, **timestamp**, **timestamp-reply**,**information-request**, **information-reply**, **address-mask-request**,**address-mask-reply**, **traceroute**, **datagram-conversion-error**,**mobile-host-redirect**, **ipv6-where-are-you**, **ipv6-i-am-here**,**mobile-registration-request**, **mobile-registration-reply**, **domain-name-request**,**domain-name-reply**, **skip** and **photuris**. (Range: 0-255)
- *icmp-code* — Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. (Range: 0-255)
- *igmp-type* — IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: **dvmrp**, **host-query**, **host-report**, **im** or **trace**. (Range: 0-255)
- *destination-port* — Specifies the UDP/TCP destination port. (Range: 0-65535)
- *source-port* — Specifies the UDP/TCP source port. (Range: 0-65535)
- *list-of-flags* — Specifies a list of TCP flags that can be triggered. If a flag is set, it is prefixed by “+”. If a flag is not set, it is prefixed by “-”. The possible values are: +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -

fin. The flags are concatenated into one string. For example: +fin-ack. To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).

Default Configuration

No IPv4 ACL is defined.

Command Mode

IP-Access List Configuration mode

User Guidelines

Use the **ip access-list** Global Configuration mode command to enable the IP-Access List Configuration mode.

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

Example

The following example shows how to define a permit statement for an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-al)# permit rsvp 192.1.1.1 0.0.0.0 any dscp 56
```

deny (IP)

The **deny** IP-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

Syntax

deny [disable-port] {any | *protocol*} **{any | {***source source-wildcard*}} **{ny |** {*destination destination-wildcard*}} **[dscp** *dscp number* **| ip-precedence** *ip-precedence*]

deny-icmp [disable-port] {any | {*source source-wildcard*}} **{any |** {*destination destination-wildcard*}} **{ny |** *icmp-type*} **{any |** *icmp-code*} **[dscp** *number* **| ip-precedence** *number*]

deny-igmp [disable-port] {any | {*source source-wildcard*}} **{any |** {*destination destination-wildcard*}} **{any |** *igmp-type*} **[dscp** *number* **| ip-precedence** *number*]

deny-tcp [disable-port] {any | {*source source-wildcard*}} **{any |** *source-port*} **{any |** {*destination destination-wildcard*}} **{any |** *destination-port*} **[dscp** *number* **| ip-precedence** *number*] **[flags** *list-of-flags*]

eny-udp [disable-port] {any | {*source source-wildcard*}} **{any |** *source-port*} **{any |** {*destination destination-wildcard*}} **{any |** *destination-port*} **[dscp** *number* **| ip-precedence** *number*]

Parameters

- **disable-port** — Specifies that the port is disabled.
- *source* — Specifies the IP address or host name from which the packet was sent. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *source-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1's in bit positions to be ignored. Specify **any** to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination* — Specifies the IP address or host name to which the packet is being sent. Specify any to indicate IP address 0.0.0.0 and mask 255.255.255.255.
- *destination-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1's in bit positions to be ignored. Specify any to indicate IP address 0.0.0.0 and mask 255.255.255.255.

- *protocol* — Specifies the abbreviated name or number of an IP protocol. (Range: 0-255). The following table lists the protocols that can be specified:

IP Protocol	Abbreviated Name	Protocol Number
Internet Control Message Protocol	icmp	1
Internet Group Management Protocol	igmp	2
IP in IP (encapsulation) Protocol	ip	4
Transmission Control Protocol	tcp	6
Exterior Gateway Protocol	egp	8
Interior Gateway Protocol	igp	9
User Datagram Protocol	udp	17
Host Monitoring Protocol	hmp	20
Reliable Data Protocol	rdp	27
Inter-Domain Policy Routing Protocol	idpr	35
Ipv6 protocol	ipv6	41
Routing Header for IPv6	ipv6-route	43
Fragment Header for IPv6	ipv6-frag	44
Inter-Domain Routing Protocol	idrp	45
Reservation Protocol	rsvp	46
General Routing Encapsulation	gre	47
Encapsulating Security Payload (50)	esp	50
Authentication Header	ah	51
ICMP for IPv6	ipv6-icmp	58
EIGRP routing protocol	eigrp	88
Open Shortest Path Protocol	ospf	89
IP-within-IP Encapsulation Protocol	ipip	94
Protocol Independent Multicast	pim	103
Layer Two Tunneling Protocol	l2tp	115

IP Protocol	Abbreviated Name	Protocol Number
ISIS over IPv4	isis	124
(any IP protocol)	any	(25504)

- **in-port port-num —** (Optional) Specifies the input port of the device. In case of egress classification this port will be the device input port.
- **out-port port-num —** (Optional) Specifies the output port of the device.
- **dscp** *number* — Indicates matching the **dscp** *number* with the packet dscp value.
- **ip-precedence** *number* — Indicates matching the **ip-precedence** *number* with the packet ip-precedence value.

Default Configuration

This command has no default configuration

Command Mode

IP-Access List Configuration mode

User Guidelines

Use the **ip access-list** Global Configuration mode command to enable the IP-Access List Configuration mode.

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the defined conditions are denied.

Example

The following example shows how to define a permit statement for an IP ACL.

```
Console(config)# ip access-list ip-acl1
Console(config-ip-al)# deny rsvp 192.1.1.1 0.0.0.255 any
```

mac access-list

The **mac access-list** Global Configuration mode command enables the MAC-Access List Configuration mode and creates Layer 2 ACLs. To delete an ACL, use the **no** form of this command.

Syntax

mac access-list *name*

no mac access-list *name*

Parameters

- *name* — Specifies the name of the ACL. (Range: 0-32 characters) Use “” for empty string.

Default Configuration

The default for all ACLs is deny all.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how to create a MAC ACL.

```
Console(config)# mac access-list macl-acl1
Console(config-mac-al)#
```

permit (MAC)

The **permit** MAC-Access List Configuration mode command defines permit conditions of an MAC ACL.

Syntax

permit {**any** | {**host** *source source-wildcard*} **any** | {*destination destination-wildcard*}} [**lan** *vlan-id*] [**cos** *cos cos-wildcard*] **thtype** *eth-type*] [**inner-vlan** *vlan-id*]

Parameters

- *source* — Specifies the source MAC address of the packet.
- *source-wildcard* — Specifies wildcard bits to be applied to the source MAC address. Use 1s in bit positions to be ignored.
- *destination* — Specifies the MAC address of the host to which the packet is being sent.
- *destination-wildcard* — Specifies wildcard bits to be applied to the destination MAC address. Use 1s in bit positions to be ignored.
- *vlan-id* — Specifies the ID of the packet vlan. (Range: 0-4094)
- *cos* — Specifies the Class of Service (CoS) for the packet. (Range: 0-7)
- *cos-wildcard* — Specifies wildcard bits to be applied to the CoS.
- *eth-type* — Specifies the Ethernet type of the packet .(Range: 05dd-ffff (hex))
- *inner-vlan vlan-id* — Specifies the inner VLAN ID of a double tagged packet

Default Configuration

No MAC ACL is defined.

Command Mode

MAC-Access List Configuration mode

User Guidelines

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied **deny-any-any** condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

If the VLAN ID is specified, the policy map cannot be connected to the VLAN interface.

Example

The following example shows how to create a MAC ACL with permit rules.

```
Console(config)# mac access-list macl-acl1
Console(config-mac-al)# permit 6:6:6:6:6:6 0:0:0:0:0:0 ny vlan 6
```

deny (MAC)

The **deny** MAC-Access List Configuration mode command denies traffic if the conditions defined in the deny statement match.

Syntax

deny [**disable-port**] {**any** | {*source source-wildcard*} {**any** | {*destination destination-wildcard*}}[**vlan** *vlan-id*]
[**cos** *cos cos-wildcard*] [**ethtype** *eth-type*]

Parameters

- **disable-port —** Indicates that the port is disabled if the statement is deny.
- *source* — Specifies the MAC address of the host from which the packet was sent.
- *source-wildcard* — (Optional for the first type) Specifies wildcard bits by placing 1's in bit positions to be ignored.
- *destination* — Specifies the MAC address of the host to which the packet is being sent.

- *destination-wildcard* —(Optional for the first type) Specifies wildcard bits by placing 1's in bit positions to be ignored.
- *vlan-id* — Specifies the ID of the packet vlan.
- *cos* — Specifies the packet's Class of Service (CoS).
- *cos-wildcard* —Specifies wildcard bits to be applied to the CoS.
- *eth-type* — Specifies the packet's Ethernet type.

Default Configuration

This command has no default configuration.

Command Mode

MAC-Access List Configuration mode

User Guidelines

MAC BPDU packets cannot be denied.

This command defines an Access Control Element (ACE). An ACE can only be removed by deleting the ACL, using the no mac access-list Global Configuration mode command. Alternatively, the Web-based interface canbe used to delete ACEs from an ACL.

Before an Access Control Element (ACE) is added to an ACL, all packets are permitted. After an ACE is added, an implied deny-any-any condition exists at the end of the list and those packets that do not match the conditions defined in the permit statement are denied.

If the VLAN ID is specified, the policy map cannot be connected to the VLAN interface.

Example

The following example shows how to create a MAC ACL with deny rules on a device.

```
Console(config)# mac access-list macl1
Console (config-mac-acl)# deny 00:00:00:00:10:00 any
```

service-policy

Apply a policy map to the input of a particular interface. Use no form in order to detach policy map from interface.

The command is available in Advanced mode only.

Syntax

service-policy input *policy-map-name*

no service-policy input

Parameters

- **input** — Use **input** *policy-map-name* to apply the specified policy-map to the input interface.
- *policy-map-name* — Up to 32 characters.

Default Configuration

This command has no default configuration.

Command Mode

Interface configuration (Ethernet, VLAN, Port-Channel)

User Guidelines

Only one policy map per interface per direction is supported.

service-acl

To control access to an interface, use the service-acl command in interface configuration mode. To remove the access control, use the no form of this command.

Syntax

service-acl input acl-name1

no service-acl input

Parameters

acl-name — Specifies an ACL to apply to the interface. Please see the usage guidelines.

Default Configuration

No ACL is assigned.

Command Mode

Interface configuration (Ethernet, Port-Channel).

Usage Guidelines

- Two ACLs of the same type can't be added to a port.
- An ACL can't be added to a port that is already bounded to an ACL, without first removing the current ACL and binding the two ACLs together.

show access-lists

The **show access-lists** Privileged EXEC mode command displays access control lists (ACLs) defined on the device.

Syntax

show access-lists [*name*]

Parameters

- *name* — The name of the ACL.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays access lists defined on a device.

```
Console# show access-lists
IP access list ACL1
permit ip host 172.30.40.1 any
permit rsvp host 172.30.8.8 any
```

show interfaces access-lists

The **show interfaces access-lists** Privileged EXEC mode command displays access lists applied on interfaces.

Syntax

show interfaces access-lists [**ethernet** interface | **port-channel** port-channel-number]

Parameters

- *interface* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays ACLs applied to the interfaces of a device:

```
Console# show interfaces access-lists

Interface      Input
---------      -----
e1             ACL1
e2             ACL3
```

4

ARP Inspection Commands

ip arp inspection

The **ip arp inspection** Global Configuration mode command globally enables ARP inspection. To disable ARP inspection, use the **no** form of this command.

Syntax

ip arp inspection

no ip arp inspection

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example globally enables ARP inspection.

```
Console(config)# ip arp inspection
```

ip arp inspection vlan

The **ip arp inspection vlan** Global Configuration mode command enables ARP inspection based on DHCP snooping database on a VLAN. To disable ARP inspection on a VLAN, use the **no** form of this command.

Syntax

ip arp inspection *vlan-id*

no ip arp inspection *vlan-id*

Parameters

- *vlan-id* — Specifies a VLAN ID.

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables ARP inspection on a VLAN based on the DHCP snooping database. The ip arp inspection list assign Global Configuration mode command enables static ARP inspection.

Example

The following example enables ARP inspection on a VLAN based on the DHCP snooping database.

```
Console(config)# ip arp inspection vlan
```

ip arp inspection trust

The **ip arp inspection trust** Interface Configuration (Ethernet, Port-channel) mode command configures an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. To return to the default configuration, use the **no** form of this command.

Syntax

ip arp inspection trust

no ip arp inspection trust

Default Configuration

The interface is untrusted.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode.

User Guidelines

The switch does not check ARP packets, which are received on the trusted interface; it simply forwards the packets.

For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the ip arp inspection log-buffer vlan Global Configuration mode command.

Example

The following example configures an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected.

```
Console(config)# interface ethernet 1
Console(config-if)# ip arp inspection trust
```

ip arp inspection validate

The **ip arp inspection validate** Global Configuration mode command performs specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to return to the default settings.

Syntax

ip arp inspection validate

no ip arp inspection validate

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode.

User Guidelines

The following are performed:

- **Source MAC**: Compare the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.
- **Destination MAC**: Compare the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses.
- **IP addresses**: Compare the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP Multicast addresses.

Example

The following example perform specific checks for dynamic Address Resolution Protocol (ARP) inspection.

```
Console(config)# ip arp inspection validate
```

ip arp inspection list create

The **ip arp inspection list create** Global Configuration mode command creates a static ARP binding list and to enter the ARP list configuration mode. To delete the list, use the **no** form of this command.

Syntax

ip arp inspection list create *name*

no ip arp inspection list create *name*

Parameters

- *name* — Specifies the list name. (Range: 1-32 characters)

Default Configuration

No static ARP binding list exists.

Command Mode

Global Configuration mode

User Guidelines

This command enables static ARP inspection on a VLAN.

Example

The following example creates a static ARP binding list and to enter the ARP list configuration mode.

```
Console(config)# ip arp inspection list create
```

ip mac

The **ip mac** ARP-list Configuration mode command displays static ARP binding. To delete a binding, use the **no** form of this command.

Syntax

ip *ip-address* **mac** *mac-address*

no ip *ip-address* **mac** *mac-address*

Parameters

- *ip-address* — Specifies the IP address to be entered to the list.
- *mac-address* — Specifies the MAC address associated with the IP address.

Default Configuration

No binding is defined.

Command Mode

ARP-list Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays static ARP binding.

```
Console(config)# ip arp inspection list servers
Console(config-ARP-list)# ip 172.16.1.1 mac 0060.704C.7321
Console(config-ARP-list)# ip 172.16.1.2 mac 0060.704C.7322
```

ip arp inspection list assign

The **ip arp inspection list assign** Global Configuration mode command assigns static ARP binding lists to a VLAN. To delete the assignment, use the **no** form of this command.

Syntax

ip arp inspection list assign *vlan-id name*

no ip arp inspection list assign *vlan*

Parameters

- *vlan-id* — Specifies the VLAN ID.
- *name* — Specifies the list name.

Default Configuration

No static ARP binding list assignment exists.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example assigns static ARP binding lists to a VLAN.

```
Console(config)# ip arp inspection list assign
```

ip arp inspection logging interval

The **ip arp inspection logging interval** Global Configuration mode command configures the minimal interval between successive ARP SYSLOG messages. To return to the default configuration, use the **no** form of this command.

Syntax

ip arp inspection logging interval {*seconds* | **infinite**}

no ip arp inspection logging interval

Parameters

- *seconds* — Specifies the minimal interval between successive ARP SYSLOG messages. A 0 value means that a system message is immediately generated. (Range: 0-86400)
- **infinite** — Specifies SYSLOG messages are not generated.

Default Configuration

The default value is 5 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the minimal interval between successive ARP SYSLOG messages.

```
Console(config)# ip arp inspection logging interval
```

show ip arp inspection

The **show ip arp inspection** EXEC mode command displays the ARP inspection configuration.

Syntax

show ip arp inspection [ethernet *interface* **| port-channel** *port-channel-number***]**

Parameters

- *interface* — Specifies an Ethernet port.
- *port-channel-number* — Specifies a port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

EXEC

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the ARP inspection configuration.

```
Console# show ip arp inspection

IP ARP inspection is enabled.
IP ARP inspection is configured on following VLANs: 2, 7-18
Verification of packet header is enabled
Syslog messages interval: 5 seconds

InterfaceTrusted
----------------
e1yes
e2no
```

show ip arp inspection list

The **show ip arp inspection list** Privileged EXEC mode command displays the static ARP binding list.

Syntax

show ip arp inspection list

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the static ARP binding list.

```
Console# show ip arp inspection list

List name: servers
Assigned to VLANs: 1,2

IP                  ARP
----------          --------------
172.16.1.1          0060.704C.7321
172.16.1.2          0060.704C.7322
```

5

Address Table Commands

bridge address

The **bridge address** Interface Configuration (VLAN) mode command adds a MAC-layer station source address to the bridge table. To delete the MAC address, use the **no** form of this command.

Syntax

```
bridge address mac-address {ethernet interface | port-channel
port-channel-number} [permanent | delete-on-reset | delete-on-
timeout | secure]

no bridge address [mac-address]
```

Parameters

- *mac-address* — A valid MAC address.
- *interface*— A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.
- **permanent** — The address can only be deleted by the **no bridge address** command.
- **delete-on-reset** — The address is deleted after reset.
- **delete-on-timeout** — The address is deleted after “age out” time has expired.
- **secure** — The address is deleted after the port changes mode to unlock learning (**no port security** command). This parameter is only available when the port is in the learning locked mode.

Default Configuration

No static addresses are defined. The default mode for an added address is **permanent**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Using the **no** form of the command without specifying a MAC address deletes all static MAC addresses belonging to this VLAN).

Example

The following example adds a permanent static MAC-layer station source address 3aa2.64b3.a245 on port 1 to the bridge table.

```
Console(config)# interface vlan 2
Console(config-if)# bridge address 3aa2.64b3.a245 ethernet e16
permanent
```

bridge multicast filtering

The **bridge multicast filtering** Global Configuration mode command enables filtering Multicast addresses. To disable filtering Multicast addresses, use the **no** form of this command.

Syntax

bridge multicast filtering

no bridge multicast filtering

Default Configuration

Filtering Multicast addresses is disabled. All Multicast addresses are flooded to all ports.

Command Mode

Global Configuration mode

User Guidelines

If Multicast devices exist on the VLAN, do not change the unregistered Multicast addresses state to drop on the switch ports.

If Multicast devices exist on the VLAN and IGMP-snooping is not enabled, the **bridge multicast forward-all** command should be used to enable forwarding all Multicast packets to the Multicast switches.

Example

In the following example, bridge Multicast filtering is enabled.

```
Console(config)# bridge multicast filtering
```

bridge multicast address

The **bridge multicast address** Interface Configuration (VLAN) mode command registers a MAC-layer Multicast address in the bridge table and statically adds ports to the group. To unregister the MAC address, use the **no** form of this command.

Syntax

bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}

bridge multicast address {*mac-multicast-address* | *ip-multicast-address*} [**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}

Parameters

- **add** — Adds ports to the group. If no option is specified, this is the default option.
- **remove** — Removes ports from the group.
- *mac-multicast-address* — A valid MAC Multicast address.
- *ip- multicast-address* — A valid IP Multicast address.
- *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

No Multicast addresses are defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

If the command is executed without add or remove, the command only registers the group in the bridge database. Static Multicast addresses can only be defined on static VLANs.

Example

The following example registers the MAC address:

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
```

The following example registers the MAC address and adds ports statically.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
add ethernet e1, e2
```

bridge multicast forbidden address

The **bridge multicast forbidden** address Interface Configuration (VLAN) mode command forbids adding a specific Multicast address to specific ports. Use the **no** form of this command to restore the default configuration.

Syntax

bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*} [**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*}

Parameters

- **add** — Adds ports to the group. If no option is specified, this is the default option.
- **remove** — Removes ports from the group.
- *mac-multicast-address* — A valid MAC Multicast address.
- *ip- multicast-address* — A valid IP Multicast address.
- *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

Example

In this example, MAC address 0100.5e02.0203 is forbidden on port e9 within VLAN 8.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
Console(config-if)# bridge multicast forbidden address
01:00:5e:02:02:03 add ethernet e9
```

bridge multicast forward-all

The **bridge multicast forward-all** Interface Configuration (VLAN) mode command enables forwarding all Multicast packets on a port. Use the **no** form of this command to restore the default configuration.

Syntax

bridge multicast forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forward-all

Parameters

- **add** — Force forwarding all Multicast packets.
- **remove** — Do not force forwarding all Multicast packets.
- *interface-list* — Separate nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separate nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

This setting is disabled

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, all Multicast packets on port e8 are forwarded.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forward-all add ethernet e8
```

bridge multicast forbidden forward-all

The b**ridge multicast forbidden forward-all** Interface Configuration (VLAN) mode command forbids a port to be a forward-all-Multicast port. Use the **no** form of this command to restore the default configuration.

Syntax

bridge multicast forbidden forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}

no bridge multicast forbidden forward-all

Parameters

- **add** — Forbids forwarding all Multicast packets.
- **remove** — Does not forbid forwarding all Multicast packets.
- *interface-list* — Separates nonconsecutive Ethernet ports with a comma and no spaces; a hyphen is used to designate a range of ports.
- *port-channel-number-list* — Separates nonconsecutive port-channels with a comma and no spaces; a hyphen is used to designate a range of port-channels.

Default Configuration

This setting is disabled

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

IGMP snooping dynamically discovers Multicast device ports. When a Multicast device port is discovered, all the Multicast packets are forwarded to it unconditionally.

This command prevents a port from becoming a Multicast device port.

Example

In this example, forwarding all Multicast packets to e1 with VLAN 2 is forbidden.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forbidden forward-all add
ethernet e1
```

bridge aging time

The **bridge aging-time** Global Configuration mode command sets the address table aging time. To restore the default configuration, use the **no** form of this command.

Syntax

bridge aging-time *seconds*

no bridge aging-time

Parameters

- *seconds* — Time in seconds. (Range: 10-630 seconds)

Default Configuration

The default setting is **300** seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

In the following example, the bridge aging time is set to 250 seconds.

```
Console(config)# bridge aging-time 250
```

clear bridge

The **clear bridge** Privileged EXEC mode command removes any learned entries from the forwarding database.

Syntax

clear bridge

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In the following example, the bridge tables are cleared.

```
Console# clear bridge
```

port security

The **port security** Interface Configuration mode command locks the port to block unknown traffic and prevent the port from learning new addresses. To restore defaults, use the **no** form of this command.

Syntax

port security [forward | discard | discard-shutdown] [trap *seconds***]**

no port security

Parameters

- **forward** — Forwards packets with unlearned source addresses, but does not learn the address.
- **discard** — Discards packets with unlearned source addresses. This is the default if no option is indicated.
- **discard-shutdown** — Discards packets with unlearned source addresses. The port is also shut down.
- *seconds* — Sends SNMP traps and defines the minimum amount of time in seconds between consecutive traps. (Range: 1-1000000)
- **max** — Maximum number of addresses that can be learned on the interface. (Range: 1-128)

Default Configuration

This setting is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, port e1 forwards all packets without learning addresses of packets from unknown sources and sends traps every 100 seconds if a packet with an unknown source address is received.

```
Console(config)# interface ethernet e1
Console(config-if)# port security forward trap 100
```

port security mode

The **port security mode** Interface Configuration mode command configures the port security mode. To restore defaults, use the **no** form of this command.

Syntax

port security mode {lock | mac-addresses}

no port security mode

Parameters

- **lock** — Saves the current dynamic MAC addresses associated with the port and disables learning, relearning and aging.
- **mac-addresses** — Deletes the current dynamic MAC addresses associated with the port and learns up to the maximum number addresses allowed on the port. Relearning and aging are enabled.

Default Configuration

This setting is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, port security mode is set to dynamic for Ethernet interface e7.

```
Console(config)# interface ethernet e7
Console(config-if)# port security mode mac-addresses
```

port security max

The **port security max** Interface Configuration mode command configures the maximum addresses that can be learned on the port while the port is in port security max-addresses mode. Use the **no** form of this command to return to default.

Syntax

port security max *max-addr*

no port security max

Parameters

- *max-addr* — Maximum number of addresses that can be learned on the port. The range is 1-128.

Default Configuration

The default configuration is 128.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

In this example the **port security max** interface configuration command configures the maximum addresses that can be learned on the port while the port is in port security max-addresses mode.

```
Console(config)# interface ethernet e7
Console(config-if)# port security max max addr
```

show bridge address-table

The **show bridge address-table** Privileged EXEC mode command displays all entries in the bridge-forwarding database.

Syntax

show bridge address-table [vlan *vlan*] **[ethernet** *interface* **|** **port-channel** *port-channel-number* **|** **address** *mac-address*]

Parameters

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.
- *mac-address* — A valid MAC address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Internal usage VLANs (VLANs that are automatically allocated on ports with a defined Layer 3 interface) are presented in the VLAN column by a port number and not by a VLAN ID.

“Special” MAC addresses that were not statically defined or dynamically learned are displayed in the MAC address table. This includes, for example, MAC addresses defined in ACLs.

Example

In this example, all classes of entries in the bridge-forwarding database are displayed

```
Console# show bridge address-table

Aging time is 300 secs

interface   mac address        Port     Type
-------------------------      ----     -------
1        00:60:70:4C:73:FF     e8       dynamic
1        00:60:70:8C:73:FF     e8       dynamic
200      00:10:0D:48:37:FF     e9       static
```

show bridge address-table static

The **show bridge address-table static** Privileged EXEC mode command displays statically created entries in the bridge-forwarding database.

Syntax

show bridge address-table static [vlan *vlan***] [ethernet** *interface* **| port-channel** *port-channel-number***]**

Parameters

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, all static entries in the bridge-forwarding database are displayed.

```
Console# show bridge address-table static

Aging time is 300 sec

vlan     mac address           port      type
----   --------------------   -----------------
1        00:60:70:4C:73:FF     e8        Permanent
1        00:60.70.8C.73:FF     e8        delete-on-timeout
200      00:10:0D:48:37:FF     e9        delete-on-reset
```

show bridge address-table count

The **show bridge address-table count** Privileged EXEC mode command displays the number of addresses present in the Forwarding Database.

Syntax

show bridge address-table count [**vlan** *vlan*] [**Ethernet** *interface-number* | **port-channel** *port-channel-number*]

Parameters

- *vlan* — Specifies a valid VLAN, such as VLAN 1.
- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

```
This command has no default configuration.
```

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, the number of addresses present in all VLANs are displayed.

```
Console# show bridge address-table count

Capacity: 8192
Free: 8083
Used: 109
```

```
Secure addresses: 2
Static addresses: 1
Dynamic addresses: 97
Internal addresses: 9
```

show bridge multicast address-table

The **show bridge multicast address-table** Privileged EXEC mode command displays Multicast MAC address or IP Address Table information.

Syntax

```
show bridge multicast address-table [vlan vlan-id] [address mac-multicast-address | ip-multicast-address] [format ip | format mac
```

Parameters

- *vlan-id* — Indicates the VLAN ID. This has to be a valid VLAN ID value.
- *mac-multicast-address* — A valid MAC Multicast address.
- *ip-multicast-address* — A valid IP Multicast address.
- **format ip / mac** — Multicast address format. Can be **ip** or **ac**. If the format is unspecified, the default is **mac**.

Default Configuration

This command has no default configuration.

Command Mode

```
Privileged EXEC mode
```

User Guidelines

A MAC address can be displayed in IP format only if it is in the range of 0100.5e00.0000-0100.5e7f.ffff.

Example

In this example, Multicast MAC address and IP Address Table information are displayed.

```
Console# show bridge multicast address-table

Vlan    MAC Address           Type      Ports

----    --------------        -------   ---------

1       01:00:5e:02:02:03     static    e1, e13

19      01:00:5e:02:02:08     static    e1-e8

19      00:00:5e:02:02:08     dynamic   e9-e11

Forbidden ports for multicast addresses:

Vlan    MAC Address           Ports

----    --------------        -----

1       01:00:5e:02:02:03     e16

19      01:00:5e:02:02:08     e16


Console# show bridge multicast address-table format ip

Vlan    IP/MAC Address        Type      Ports

----    -----------------     -------   ---------

1       224-239.130|2.2.3     static    e1, e13

19      224-239.130|2.2.8     static    e1-e8

19      224-239.130|2.2.8     dynamic   e9-e11

Forbidden ports for multicast addresses:

Vlan    IP/MAC Address        Ports

----    --------------        -----

1       224-239.130|2.2.3     e16

19      224-239.130|2.2.8     e16
```

NOTE A Multicast MAC address maps to multiple IP addresses as shown above.

show bridge multicast address-table static

The **show bridge multicast address-table static** Privileged EXEC mode command displays the statically configured Multicast addresses.

Syntax

show bridge multicast address-table static [**vlan** *vlan-id*] [**address** *mac-multicast-address* | *ip-multicast-address*]
[**source** *ip-address*]

Parameters

- *vlan-id* — Indicates the VLAN ID. This has to be a valid VLAN ID value.
- *mac-multicast-address* — A valid MAC Multicast address.
- *ip-multicast-address* — A valid IP Multicast address.
- *ip-address* — Source IP address.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is in the range 0100.5e00.0000 through 0100.5e7f.ffff.

Example

```
Console# show bridge multicast address-table static

MAC-GROUP Table

Vlan    MAC Address         Type     Ports
----    --------------      -------  -----------
1       0100.9923.8787      static   e1, e2

Forbidden ports for Multicast addresses:

Vlan    MAC Address         Ports
----    --------------      -----
```

show bridge multicast filtering

The **show bridge multicast filtering** Privileged EXEC mode command displays the Multicast filtering configuration.

Syntax

show bridge multicast filtering *vlan-id*

Parameters

- *vlan-id* — Indicates the VLAN ID. This has to be a valid VLAN ID value.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, the Multicast configuration for VLAN 1 is displayed.

```
Console# show bridge multicast filtering 1

Filtering: Enabled
VLAN: 1

Port    Static       Status
----    ---------    ---------
e1                   Filter
e2                   Filter
e3                   Filter
```

show ports security

The **show ports security** Privileged EXEC mode command displays the port-lock status.

Syntax

show ports security [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In this example, all classes of entries in the port-lock status are displayed:

```
Console# show ports security

Port  Status  Learning  Action    Maximum   Trap  Frequency
----  ------  --------  ------    -------   ----  ---------
e1            Locked    Dynamic   Discard   3     Enable100
e2            Unlocked  Dynamic   -                   28--
e3            Locked    Disabled  Discard,  8     Disable-
                                                  Shutdown
```

The following table describes the fields shown above.

Field	Description
Port	The port number
Status	The values are: Locked, Unlocked
Learning	The learning mode
Action	Action on violation
Maximum	The maximum number of addresses that can be associated on this port in the Static Learning mode or in the Dynamic Learning mode.
Traps	Sends traps in case of a violation.
Frequency	The minimum time interval between consecutive traps.

show ports security addresses

The **show ports security addresses** Privileged EXEC mode command displays the current dynamic addresses in locked ports.

Syntax

show ports security addresses [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

This example displays dynamic addresses in all currently locked ports.

```
Console# show ports security addresses

Port   Status     Learning        Current   Maximum
----   --------   --------        -------   -------
e1     Disabled   Lock            -         1
e2     Disabled   Lock            -         1
e3     Enabled    Max-addresses   0         1
```

```
e4    Port is a member in port-channel ch1
e5    Disabled   Lock            -        1
e6    Enabled    Max-addresses  0        10
ch1   Enabled    Max-addresses  0        50
ch2   Enabled    Max-addresses  0        128
```

This example displays dynamic addresses in the currently locked port e1.

```
Console# show ports security addresses ethernet e1

Port  Status      Learning    Current     Maximum
----  --------    --------    -------     -------
e1    Disabled    Lock        -           1
```

6

Clock Commands

clock set

The **clock set** Privileged EXEC mode command manually sets the system clock.

Syntax

clock set *hh:mm:ss day month year*

or

clock set *hh:mm:ss month day year*

Parameters

- *hh:mm:ss* — Current time in hours (military format), minutes, and seconds. (hh: 0-23, mm: 0-59, ss: 0-59)
- *day* — Current day (by date) in the month. (Range: 1-31)
- *month* — Current month using the first three letters by name. (Range: Jan, ..., Dec)
- *year* — Current year. (Range: 2000-2097)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the system time to 13:32:00 on March 7th, 2005.

```
Console# clock set 13:32:00 7 Mar 2005
```

clock source

The **clock source** Global Configuration mode command configures an external time source for the system clock. Use the **no** form of this command to disable external time source.

Syntax

clock source {sntp}

no clock source

Parameters

- **sntp** — SNTP servers

Default Configuration

No external clock source

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures an external time source for the system clock.

```
Console(config)# clock source sntp
```

clock timezone

The **clock timezone** Global Configuration mode command sets the time zone for display purposes. Use the **no** form of this command to set the time to the Coordinated Universal Time (UTC).

Syntax

clock timezone *hours-offset* [**minutes** *minutes-offset*] [**zone** *acronym*]

no clock timezone

Parameters

- *hours-offset* — Hours difference from UTC. (Range: -12 hours to +13 hours)
- *minutes-offset* — Minutes difference from UTC. (Range: 0-59)
- *acronym* — The acronym of the time zone. (Range: Up to 4 characters)

Default Configuration

Offset is 0.

Acronym is empty.

Command Mode

Global Configuration mode

User Guidelines

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Example

The following example sets the time zone to 6 hours difference from UTC.

```
Console(config)# clock timezone -6 zone CST
```

clock summer-time

The **clock summer-time** Global Configuration mode command configures the system to automatically switch to summer time (daylight saving time). Use the **no** form of this command to configure the software not to automatically switch to summer time.

Syntax

clock summer-time recurring {**usa** | **eu** | {*week day month hh:mm week day month hh:mm*}} [**offset** *offset*] [**one** *acronym*]

clock summer-time date *date month year hh:mm date month year hh:mm* [**offset** *offset*] [**zone** *acronym*]

clock summer-time date *month date year hh:mm month date year hh:mm* [**offset** *offset*] [**zone** *acronym*]

no clock summer-time recurring

Parameters

- **recurring** — Indicates that summer time should start and end on the corresponding specified days every year.
- **date** — Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
- **usa** — The summer time rules are the United States rules.

- **eu** — The summer time rules are the European Union rules.
- week — Week of the month. (Range: 1-5, first, last)
- *day* — Day of the week (Range: first three letters of name; for example, **sun**)
- *date* — Date of the month. (Range:1-31)
- *month* — Month. (Range: first three letters of name; for example, **Jan**)
- *year* — year - no abbreviation (Range: 2000-2097)
- *hh:mm* — Time in military format, in hours and minutes. (Range: hh: 0-23, mm:0-59)
- *offset* — Number of minutes to add during summer time. (Range: 1-1440)
- *acronym* — The acronym of the time zone to be displayed when summer time is in effect. (Range: Up to 4 characters)

Default Configuration

Summer time is disabled.

offset — Default is 60 minutes.

acronym — If unspecified, defaults to the time zone acronym.

If the time zone has not been defined, the default is UTC.

Command Mode

Global Configuration mode

User Guidelines

In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

USA rule for daylight savings time:

- Start: Second Sunday in March
- End: First Sunday in November
- Time: 2 am local time

EU rule for daylight savings time:

- Start: Last Sunday in March
- End: Last Sunday in October
- Time: 1.00 am (01:00)

Example

The following example sets summer time starting on the first Sunday in April at 2 am and finishing on the last Sunday in October at 2 am.

```
Console(config)# clock summer-time recurring first sun apr 2:00
last sun oct 2:00
```

sntp authentication-key

The **sntp authentication-key** Global Configuration mode command defines an authentication key for Simple Network Time Protocol (SNTP). Use the **no** form of this command to remove the authentication key for SNTP.

Syntax

sntp authentication-key *number* **md5** *value*

no sntp authentication-key *number*

Parameters

- *number* — Key number (Range: 1-4294967295)
- *value* — Key value (Range: 1-8 characters)

Default Configuration

No authentication key is defined.

Command Mode

Global Configuration mode

User Guidelines

Multiple keys can be generated.

Example

The following example defines the authentication key for SNTP.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
```

sntp authenticate

The **sntp authenticate** Global Configuration mode command grants authentication for received Simple Network Time Protocol (SNTP) traffic from servers. Use the **no** form of this command to disable the feature.

Syntax

sntp authenticate

no sntp authenticate

Default Configuration

No authentication

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both Unicast and Broadcast.

Example

The following example defines the authentication key for SNTP and grants authentication.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
```

sntp port

To specify the Simple Network Time Protocol (SNTP) UDP port of the SNTP server, use the sntp port global configuration command. To use the default port, use the no form of this command.

Syntax

sntp port *port-number*

no sntp port

Parameters

- *port-number* — Port number for use by SNTP. Range: 1 - 65535

Default Configuration

123

Command Mode

Global configuration

User Guidelines

The command can change the SNTP UDP port.

Example

```
Console(config)# sntp port 12555
```

sntp trusted-key

The **sntp trusted-key** Global Configuration mode command authenticates the identity of a system to which Simple Network Time Protocol (SNTP) will synchronize. Use the **no** form of this command to disable authentication of the identity of the system.

Syntax

sntp trusted-key *key-number*

no sntp trusted-key *key-number*

Parameters

- *key-number* — Key number of authentication key to be trusted. (Range: 1-4294967295)

Default Configuration

No keys are trusted.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both received Unicast and Broadcast.

If there is at least 1 trusted key, then unauthenticated messages will be ignored.

Example

The following example authenticates key 8.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
```

sntp client poll timer

The **sntp client poll timer** Global Configuration mode command sets the polling time for the Simple Network Time Protocol (SNTP) client. Use the **no** form of this command to restore default configuration.

Syntax

sntp client poll timer *seconds*

no sntp client poll timer

Parameters

- *seconds* — Polling interval in seconds. (Range: 60-86400)

Default Configuration

Polling interval is 1024 seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the polling time for the SNTP client to 120 seconds.

```
Console(config)# sntp client poll timer 120
```

sntp broadcast client enable

The **sntp broadcast client enable** Global Configuration mode command enables Simple Network Time Protocol (SNTP) Broadcast clients. Use the **no** form of this command to disable SNTP Broadcast clients.

Syntax

sntp broadcast client enable

no sntp broadcast client enable

Default Configuration

The SNTP Broadcast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp client enable (Interface)** Interface Configuration mode command to enable the SNTP client on a specific interface.

Example

The following example enables the SNTP Broadcast clients.

```
Console(config)# sntp broadcast client enable
```

sntp anycast client enable

The **sntp anycast client enable** Global Configuration mode command enables SNTP Anycast client. Use the **no** form of this command to disable the SNTP Anycast client.

Syntax

sntp anycast client enable

no sntp anycast client enable

Default Configuration

The SNTP Anycast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Polling time is determined by the **sntp client poll timer** Global Configuration mode command.

Use the **sntp client enable (Interface)** Interface Configuration mode command to enable the SNTP client on a specific interface.

Example

The following example enables SNTP Anycast clients.

```
console(config)# sntp anycast client enable
```

sntp client enable

The **sntp client enable** Global Configuration mode command enables the Simple Network Time Protocol (SNTP) Broadcast and Anycast client on an interface. Use the **no** form of this command to disable the SNTP client.

Syntax

sntp client enable { vlan *vlan-id* **} [ethernet** interface**| port-channel** port-channel-number**]**

no sntp client enable {vlan *vlan-id***} [ethernet** interface | **port-channel** port-channel-number**]**

Parameters

- *vlan-id* — VLAN number
- *interface* — Valid Ethernet port
- *port-channel-number* — Valid port-channel number

Default Configuration

The SNTP Anycast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp broadcast client enable** Global Configuration mode command to enable Broadcast clients globally.

Use the **sntp anycast client enable** Global Configuration mode command to enable Anycast clients globally.

Example

The following example enables the Simple Network Time Protocol (SNTP) Broadcast and Anycast client on an interface.

```
console(config)# sntp client enable
```

sntp client enable (Interface)

The **sntp client enable** Interface Configuration (Ethernet, port-channel, VLAN) mode command enables the Simple Network Time Protocol (SNTP) client on an interface. This applies to both receive Broadcast and Anycast updates. Use the **no** form of this command to disable the SNTP client.

Syntax

sntp client enable

no sntp client enable

Default Configuration

The SNTP client is disabled on an interface.

Command Mode

Interface Configuration (Ethernet, port-channel, VLAN) mode

User Guidelines

Use the **sntp broadcast client enable** Global Configuration mode command to enable Broadcast clients globally.

Use the **sntp anycast client enable** Global Configuration mode command to enable Anycast clients globally.

Example

The following example enables the SNTP client on Ethernet port e3.

```
Console(config)# interface ethernet e3
Console(config-if)# sntp client enable
```

sntp unicast client enable

The **sntp unicast client enable** Global Configuration mode command enables the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers. Use the **no** form of this command to disable requesting and accepting SNTP traffic from servers.

Syntax

sntp unicast client enable

no sntp unicast client enable

Default Configuration

The SNTP Unicast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp server** Global Configuration mode command to define SNTP servers.

Example

The following example enables the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from servers.

```
Console(config)# sntp unicast client enable
```

sntp unicast client poll

The **sntp unicast client poll** Global Configuration mode command enables polling for the Simple Network Time Protocol (SNTP) predefined Unicast servers. Use the **no** form of this command to disable the polling for SNTP client.

Syntax

sntp unicast client poll

no sntp unicast client poll

Default Configuration

Polling is disabled.

Command Mode

Global Configuration mode

User Guidelines

Polling time is determined by the **sntp client poll timer** Global Configuration mode command.

Example

The following example enables polling for SNTP predefined Unicast clients.

```
Console(config)# sntp unicast client poll
```

sntp server

The **sntp server** Global Configuration mode command configures the device to use the Simple Network Time Protocol (SNTP) to request and accept SNTP traffic from a specified server. Use the **no** form of this command to remove a server from the list of SNTP servers.

Syntax

sntp server {*ip-address* | *hostname*} [**oll**] [**key** *keyid*]

no sntp server host

Parameters

- *ip-address* — IP address of the server.
- *hostname* — Hostname of the server. (Range: 1-158 characters; Maximum label size: 63)
- **poll** — Enable polling.
- *keyid* — Authentication key to use when sending packets to this peer. (Range:1-4294967295)

Default Configuration

No servers are defined.

Command Mode

Global Configuration mode

User Guidelines

Up to 8 SNTP servers can be defined.

Use the **sntp unicast client enable** Global Configuration mode command to enable predefined Unicast clients globally.

To enable polling you should also use the **sntp unicast client poll** Global Configuration mode command for global enabling.

Polling time is determined by the **sntp client poll timer** Global Configuration mode command.

Example

The following example configures the device to accept SNTP traffic from the server on 192.1.1.1.

```
Console(config)# sntp server 192.1.1.1
```

show clock

The **show clock** Privileged EXEC mode command displays the time and date from the system clock.

Syntax

show clock [detail]

Parameters

- **detail** — Shows time zone and summertime configuration.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The symbol that precedes the show clock display indicates the following information:

Symbol	Description
*	Time is not authoritative.
(blank)	Time is authoritative.
.	Time is authoritative, but SNTP is not synchronized.

Example

The following example displays the time and date from the system clock.

```
Console# show clock
15:29:03 PDT(UTC-7) Jun 17 2005
Time source is SNTP

Console# show clock detail
15:29:03 PDT(UTC-7) Jun 17 2005
Time source is SNTP

Time zone:
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.
```

show sntp configuration

The **show sntp configuration** Privileged EXEC mode command shows the configuration of the Simple Network Time Protocol (SNTP).

Syntax

show sntp configuration

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the current SNTP configuration of the device.

```
Console# show sntp configuration

Polling interval: 1024 seconds

MD5 Authentication keys: 8, 9
Authentication is required for synchronization.
Trusted Keys: 8, 9

Unicast Clients Polling: Enabled

Server           Polling       Encryption Key
------------     -------       --------------

176.1.1.8        Enabled       9
176.1.8.179      Disabled      Disabled
```

```
Broadcast Clients: Enabled
Anycast Clients: Enabled
Broadcast Interfaces: e1, e3
```

show sntp status

The **show sntp status** Privileged EXEC mode command shows the status of the Simple Network Time Protocol (SNTP).

Syntax

show sntp status

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows the status of the SNTP.

```
Console# show sntp status
```

```
Clock is synchronized, stratum 4, reference is 176.1.1.8,
unicast
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5
1993)
```

```
Unicast servers:

Server      Status   Last response                  Offset   Delay

                                                    [mSec]   [mSec]

---------- -------  ---------------------------------- ------
176.1.1.8   Up       19:58:22.289 PDT Feb 19 2005 7.33   117.79
176.1.8.179 Unknown  12:17.17.987 PDT Feb 19 2005 8.98   189.19

Anycast server:

Server     InterfaceStatus Last response          Offset Delay

                                                  [mSec] [mSec]

------------------------- -----------------------------------
176.1.11.8VLAN 118  Up     9:53:21.789 PDT Feb 19 2005 7.19  119.89

Broadcast:

Interface  IP Address     Last response

---------  ----------     ---------------------------
e13        0.0.0.0        00:00:00.0 Feb 19 2005
vlan 1     16.1.1.200     15:15:16.0 LLBG Feb 19 2006
```

7

Configuration and Image File Commands

copy

The **copy** Privileged EXEC mode command copies files from a source to a destination.

Syntax

copy *source-url destination-url* [**snmp**]

Parameters

- *source-url* — The source file location URL or reserved keyword of the source file to be copied. (Range: 1-160 characters)
- *destination-url* — The destination file URL or reserved keyword of the destination file. (Range: 1-160 characters)
- **snmp** — Used only when copying from/to startup-config. Specifies that the destination/source file is in SNMP format.

The following table displays keywords and URL prefixes.

Keyword	Source or Destination
running-config	Represents the current running configuration file
startup-config	Represents the startup configuration file.
image	If the source file, it represents the active image file. If the destination file, it represents the non-active image file.

Keyword	Source or Destination
boot	Boot file.
tftp://	Source or destination URL for a TFTP network server. The syntax for this alias is **tftp:***//host/[directory]/filename*. The host can be represented by its IP address or hostname.
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
null:	Null destination for copies or files. A remote file can be copied to null to determine its size.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The location of a file system dictates the format of the source or destination URL.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

*.prv and *.sys files cannot be copied.

Understanding Invalid Combinations of Source and Destination — Some invalid combinations of source and destination exist. Specifically, you cannot copy if one of these conditions exists:

- The source file and destination file are the same file.
- **xmodem**: is the destination file. The source file can be copied to image, boot and null: only.
- **tftp://** is the source file and destination file on the same copy.

The following table describes copy characters:

Character	Description
!	For network transfers, indicates that the copy process is taking place. Each exclamation point indicates successful transfer of ten packets (512 bytes each).
.	For network transfers, indicates that the copy process timed out. Generally, many periods in a row means that the copy process may fail.

Copying an Image File from a Server to Flash Memory — To copy an image file from a server to flash memory, use the **copy** *source-url* **image** command.

Copying a Boot File from a Server to Flash Memory — To copy a boot file from a server to flash memory, enter the **copy** *source-url* **boot** command.

Copying a Configuration File from a Server to the Running Configuration File — To load a configuration file from a network server to the running configuration file of the device, enter the **copy** *source-url* **running-config** command. The commands in the loaded configuration file are added to those in the running configuration file as if the commands were typed in the command-line interface (CLI). Thus, the resulting configuration file is a combination of the previous running configuration and the loaded configuration files with the loaded configuration file taking precedence.

Copying a Configuration File from a Server to the Startup Configuration — To copy a configuration file from a network server to the startup configuration file of the device, enter **copy** *source-url* **startup-config.** The startup configuration file is replaced by the copied configuration file.

Storing the Running or Startup Configuration on a Server — Use the **copy running-config** *destination-url* command to copy the current configuration file to a network server using TFTP. Use the **copy startup-config** *destination-url* command to copy the startup configuration file to a network server.

Saving the Running Configuration to the Startup Configuration — To copy the running configuration to the startup configuration file, enter the **copy running-config startup-config** command.

Example

The following example copies system image file1 from the TFTP server 172.16.101.101 to a non-active image file.

```
Console# copy tftp://172.16.101.101/file1 image
```

```
Accessing file ‘file1’ on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

delete startup-config

The **delete startup-config** Privileged EXEC mode command deletes the startup-config file.

Syntax

delete startup-config

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- There are no user guidelines for this command.

Examples

The following example deletes the startup-config file.

```
Console# delete startup-config
```

show running-config

The **show running-config** Privileged EXEC mode command displays the contents of the currently running configuration file.

Syntax

show running-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

- **show running-config** does not show all the port configurations under the port. Although the device is already configured with some default parameters, 'show running config' on an empty device is empty.

Examples

The following example displays the contents of the running-config file.

```
Console# show running-config
```

```
no spanning-tree
vlan database
vlan 2
```

```
exit
interface range ethernet g(1-2)
switchport access vlan 2
exit
interface vlan 2
bridge address 00:00:00:00:00:01 ethernet g1
exit
interface ethernet g1
gvrp enable
exit
gvrp enable
interface ethernet g24
ip address dhcp
exit
ip name-server  10.6.1.36
console#
```

show startup-config

The **show startup-config** Privileged EXEC mode command displays the contents of the startup configuration file.

Syntax

show startup-config

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the contents of the running configuration file.

```
Console# show startup-config

hostname device

interface ethernet e1
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000

interface ethernet e2
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
```

8

DHCP Commands

ip dhcp snooping

The **ip dhcp snooping** Global Configuration mode command globally enables DHCP snooping. Use the **no** form of this command to return to the default configuration.

Syntax

ip dhcp snooping

no ip dhcp snooping

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode

User Guidelines

For any DHCP snooping configuration to take effect, DHCP snooping must be globally enable. DHCP snooping is not active until you enable snooping on a VLAN by using the **ip dhcp snooping vlan** Global Configuration mode command.

Example

The following example enables DHCP snooping.

```
Console(config)# ip dhcp snooping
```

ip dhcp snooping vlan

The **ip dhcp snooping vlan** Global Configuration mode command enables DHCP snooping on a VLAN. Use the **no** form of this command to disable DHCP snooping on a VLAN.

Syntax

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping *vlan-id*

Parameters

- *vlan-id* — Specifies the VLAN ID.

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP snooping must first be globally enable before enabling DHCP snooping on a VLAN.

Example

The following example enables DHCP snooping on a VLAN.

```
Console(config)# ip dhcp snooping vlan
```

ip dhcp snooping trust

The **ip dhcp snooping trust** Interface Configuration (Ethernet, Port-channel) mode command configures a port as trusted for DHCP snooping purposes. Use the **no** form of this command to return to the default configuration.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Default Configuration

The interface is untrusted.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

Configure as trusted ports: Ports that are connected to a DHCP server or to other switches or routers.
Configure as untrusted ports: Ports that are connected to DHCP clients.

Example

The following example configures a port as trusted for DHCP snooping purposes.

```
Console(config)# interface ethernet 1
Console(config-if)# ip dhcp snooping trust
```

ip dhcp information option allowed-untrusted

The **ip dhcp information option allowed-untrusted** Global Configuration mode command on a switch configures it to accept DHCP packets with option-82 information from an untrusted port. Use the **no** form of this command to configure the switch to drop these packets from an untrusted port.

Syntax

ip dhcp information option allowed-untrusted

no ip dhcp information option allowed-untrusted

Default Configuration

Discard DHCP packets with option-82 information from an untrusted port.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the switch to accept DHCP packets with option-82 information from an untrusted port

```
Console(config)# ip dhcp information option allowed-untrusted
```

ip dhcp snooping verify

The **ip dhcp snooping verify** Global Configuration mode command configures the switch to verify, on an untrusted port, that the source MAC address in a DHCP packet matches the client hardware address. Use the **no** form of this command to configure the switch to not verify the MAC addresses.

Syntax

ip dhcp snooping verify

no ip dhcp snooping verify

Default Configuration

The switch verifies the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the switch to verify, on an untrusted port, that the source MAC address in a DHCP packet matches the client hardware address.

```
Console(config)# ip dhcp snooping verify
```

ip dhcp snooping database

The **ip dhcp snooping database** Global Configuration mode command configures the DHCP snooping binding file. Use the **no** form of this command to delete the binding file.

Syntax

ip dhcp snooping database

no ip dhcp snooping database

Default Configuration

The URL is not defined.

Command Mode

Global Configuration mode

User Guidelines

To ensure that the lease time in the database is accurate and the Simple Network Time Protocol (SNTP) is enabled and configured.

The switch writes binding changes to the binding file only when the switch system clock is synchronized with SNTP.

Example

The following example configures the DHCP snooping binding file.

```
Console(config)# ip dhcp snooping database
```

ip dhcp snooping database update-freq

The **ip dhcp snooping database update-freq** Global Configuration Command configures the update frequency of the DHCP snooping binding file. Use the **no** form of this command to return to the default configuration.

Syntax

ip dhcp snooping database update-freq *seconds*

no ip dhcp snooping database update-freq

Parameters

- *seconds* — Specifies, in seconds, the update frequency. (Range: 600 – 86400)

Default Configuration

The default value is **1200**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the update frequency of the DHCP snooping binding file.

```
Console(config)# ip dhcp snooping database update-freq 600
```

ip dhcp snooping binding

The **ip dhcp snooping binding** Privileged EXEC mode command configures the DHCP snooping binding database and adds binding entries to the database. Use the **no** form of this command to delete entries from the binding database.

Syntax

ip dhcp snooping binding *mac-address vlan-id ip-address* {**ethernet** *interface* | **port-channel** *port-channel-number*} **xpiry** *seconds*

no ip dhcp snooping binding *mac-address vlan-id*

Parameters

- *mac-address* — Specifies a MAC address.
- *vlan-id* — Specifies a VLAN number.
- *ip-address* — Specifies an IP address.
- *interface* — Specifies an Ethernet port.
- *port-channel-number* — Specifies the Port-channel number.
- **expiry** *seconds* — Specifies the interval, in seconds, after which the binding entry is no longer valid. (Range: 10 – 4294967295)

Default Configuration

No static binding exists.

Command Mode

Privileged EXEC mode

User Guidelines

After entering this command an entry is added to the DHCP snooping database. If DHCP snooping binding file exists, the entry is added to that file also.

The entry is displayed in the show commands as a “DHCP Snooping entry”.

Example

The following example configures the DHCP snooping binding database and adds binding entries to the database.

```
Console(enable)# ip dhcp snooping binding
```

clear ip dhcp snooping database

The **clear ip dhcp snooping database** Privileged EXEC mode command clears the DHCP binding database.

Syntax

clear ip dhcp snooping database

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears the DHCP binding database.

```
Console(enable)# clear ip dhcp snooping binding
```

show ip dhcp snooping

The **show ip dhcp snooping** Privileged EXEC mode command displays the DHCP snooping configuration.

Syntax

show ip dhcp snooping [ethernet *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Specifies the Ethernet port.
- *port-channel-number* — Specifies the Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the DHCP snooping configuration.

```
Console# show ip dhcp snooping

DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 2, 7-18
DHCP snooping database: enabled
Option 82 on untrusted port is allowed
Relay agent information option 82 is enabled.
Verification of hwaddr field is enabled
```

```
Interface              Trusted
----------------       ----------------
e1                     Yes
e2                     Yes
```

show ip dhcp snooping binding

The **show ip dhcp snooping binding** Privileged EXEC mode command displays the DHCP snooping binding database and configuration information for all interfaces on a switch.

Syntax

show ip dhcp snooping binding [**mac-address** *mac-address*] [**ip-address** *ip-address*] [**vlan** *vlan-id*] [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *mac-address* — Specifies a MAC address.
- *ip-address* — Specifies an IP address.
- *vlan-id* — Specifies a VLAN number.
- *interface* — Specifies an Ethernet port.
- *port-channel-number* — Specifies the Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the DHCP snooping binding database and configuration information for all interfaces on a switch.

```
Console# show ip dhcp snooping binding
Update frequency: 1200
Total number of binding: 3

Mac Address     IP Address Lease    Type       VLAN  Interface
                           (sec)

-----------     ---------- -------- ---------- ----  ----------
0060.704C.73FF  10.1.8.1   7983     snooping   3     e21
10060.704C.7BC1 10.1.8.2   92332    snooping   3     e22
                                    (s)
```

9

DHCP Relay Commands

ip dhcp relay enable (global)

The **ip dhcp relay enable** Global Configuration mode command enables Dynamic Host Configuration Protocol (DHCP) relay features on your router. Use the **no** form of this command to disable the relay agent features.

Syntax

ip dhcp relay enable

no ip dhcp relay enable

Default Configuration

DHCP is disabled on the router.

Command Mode

Global (Interface) Configuration mode

User Guidelines

This command is only functional if the device is in Router mode.

Example

The following example enables DHCP services on the DHCP Server.

```
Console(config)# ip dhcp relay enable
```

ip dhcp relay enable (interface)

The **ip dhcp relay enable** Interface Configuration mode command enables Dynamic Host Configuration Protocol (DHCP) relay features for an interface. Use the **no** form of this command to disable the relay agent features.

Syntax

ip dhcp relay enable

no ip dhcp relay enable

Default Configuration

For a switch: Disabled.

Command Mode

For a switch: Interface Configuration (VLAN) mode

User Guidelines

DHCP relay must be enabled before enabling DHCP snooping on an interface.

Example

The following example enables DHCP services on the DHCP Server.

```
Console(config-if)# ip dhcp relay enable
```

ip dhcp relay address

The **ip dhcp relay address** Global Configuration mode command defines the DHCP servers that are available for DHCP relay. Use the **no** form of this command to remove a server from the available DHCP servers list.

Syntax

ip dhcp relay address *ip-address*

no ip dhcp relay address [*ip-address*]

Parameters

- *ip-address* — DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Global Configuration mode

User Guidelines

If no IP address is specified when using the **no** form of the command, all configured servers are removed.

Example

The following example defines the DHCP server with address 172.16.1.1 to be available for DHCP relay.

```
Console(config-if)# ip dhcp relay address 172.16.1.1
```

show ip dhcp relay

The **show ip dhcp relay** Privileged EXEC mode command displays the defined DHCP relay server addresses available for DHCP relay.

Syntax

show ip dhcp relay

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command is only functional if the device is in Router mode.

Example

The following example displays DHCP relay server addresses.

```
Console# show ip dhcp relay
DHCP relay is enabled.
Servers: 172.16.1.11, 172.16.8.11
```

10

DHCP Option 82 Commands

ip dhcp information option

The **ip dhcp information option** Global Configuration mode command enables DHCP option-82 data insertion. Use the **no** form of this command to disable DHCP option-82 data insertion.

Syntax

ip dhcp information option

no ip dhcp information option

Default Configuration

DHCP option-82 data insertion is enabled.

Command Mode

Global Configuration mode.

User Guidelines

DHCP option 82 is enabled when DHCP snooping is enabled on VLANs.

Example

The following example configures the update frequency of the DHCP snooping binding file.

```
Console(config)# ip dhcp information option
```

show ip dhcp information option

The **show ip dhcp information option** Privileged EXEC command displays the DHCP option 82 configuration.

Syntax

show ip dhcp information option

Default Configuration

No default configuration for this command.

Command Mode

Privileged EXEC mode.

User Guidelines

DHCP option 82 is enabled when DHCP snooping is enabled on VLANs.

Example

The following example configures the update frequency of the DHCP snooping binding file.

```
Console# show ip dhcp information option
Relay agent information option 82 is enabled
```

11

DHCP Auto-configuration

ip dhcp autoconfig

To enable the support of auto configuration via DHCP option 67 field, use the **ip dhcp autoconfig** global configuration command. To disable DHCP auto configuration, use the **no** form of this command.

Syntax

ip dhcp autoconfig

no ip dhcp autoconfig

Command Mode

Global configuration

Default Configuration

By default the feature is enabled

Usage Guidelines

The command enables the support of auto-configuration via DHCP option 67 field. The DHCP server should be provisioned with the configuration file URL in a TFTP server. The configuration data is set to the device upon IP renewal (for example, reboot) and once loaded the device would reset itself.

ip dhcp autoconfig file

To manually set the file name for auto configuration via DHCP option 67 field, use the **ip dhcp autoconfig** file global configuration command. To delete the auto configuration filename, use the **no** form of this command.

Syntax

ip dhcp autoconfig file *filename*

no ip dhcp autoconfig file

Parameters

- *filename* — Auto-configuration file name (up to 160 characters).

Command Mode

Global configuration

Default Configuration

By default the filename is null

Usage Guidelines

The command sets the auto-configuration filename. Normally the name is received via DHCP option 67 procedure from the DHCP server, when auto config is enabled. Since auto-configuration takes place only when the configuration file is changed, the no command can be used to erase the configuration file to force auto-configuration or the command may set a specific configuration name as in the DHCP server to prevent the auto-configuration procedure.

show ip dhcp autoconfig

To show the status of the IP DHCP autoconfig mode use the show ip dhcp autoconfig EXEC command.

Syntax

show ip dhcp autoconfig

Command Mode

EXEC

Example

```
Device# show ip dhcp autoconfig

DHCP autoconfig enabled
Ip dhcp autoconfig filename /config/configfile1.txt
```

12

Ethernet Configuration Commands

interface ethernet

The **interface ethernet** Global Configuration mode command enters the interface configuration mode to configure an Ethernet type interface.

Syntax

interface ethernet *interface*

Parameters

- *interface* — Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables configuring Ethernet port e18.

```
Console(config)# interface ethernet e18
```

interface range ethernet

The **interface range ethernet** Global Configuration mode command configures multiple Ethernet type interfaces at the same time.

Syntax

interface range ethernet {*port-list* | **all**}

Parameters

- *port-list* — List of valid ports. Where more than one port is listed, separate the nonconsecutive ports with a comma and no spaces, use a hyphen to designate a range of ports and group a list separated by commas in brackets.
- **all** — All Ethernet ports.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each active interface in the range. If the command returns an error on one of the active interfaces, it does not stop executing commands on other active interfaces.

Example

The following example shows how ports e18 to e20 and e1 to e12 are grouped to receive the same command.

```
Console(config)# interface range ethernet e18-e20,e1-e12
Console(config-if)#
```

shutdown

The **shutdown** Interface Configuration (Ethernet, port-channel) mode command disables an interface. Use the **no** form of this command to restart a disabled interface.

Syntax

shutdown

no shutdown

Default Configuration

The interface is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables Ethernet port e5 operations.

```
Console(config)# interface ethernet e5
Console(config-if)# shutdown
```

The following example restarts the disabled Ethernet port.

```
Console(config)# interface ethernet e5
Console(config-if)# no shutdown
```

description

The **description** Interface Configuration (Ethernet, port-channel) mode command adds a description to an interface. Use the **no** form of this command to remove the description.

Syntax

description *string*

no description

Parameters

- *string* — A comment or a description of the port to allow the user to remember the purpose of the interface. (Range: 1-64 characters)

Default Configuration

The interface does not have a description.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds a description to Ethernet port e5.

```
Console(config)# interface ethernet e5
Console(config-if)# description “RD SW#3”
```

speed

The **speed** Interface Configuration (Ethernet, port-channel) mode command configures the speed of a given Ethernet interface when not using auto-negotiation.

NOTE To configure the speed of a fiber SFP port, use the **sfp speed** command.

Syntax

speed {**10** | **100** | **1000**| **10000**}

Parameters

- **10** — Forces 10 Mbps operation.
- **100** — Forces 100 Mbps operation.
- **1000** — Forces 1000 Mbps operation.
- **10000** — Forces 10000 Mbps operation.

Default Configuration

Maximum port capability: 38400

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the speed operation of Ethernet port e5 to 100 Mbps operation.

```
Console(config)# interface ethernet e5
Console(config-if)# speed 100
```

duplex

The **duplex** Interface Configuration (Ethernet) mode command configures the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. Use the **no** form of this command to restore the default configuration.

NOTE (SPS224G4 combo ports) This command applies when the copper port is used. The configuration does not apply when an SFP is plugged to the port.

Syntax

duplex {**half** | **full**}

no duplex

Parameters

- **half** — Forces half-duplex operation
- **full** — Forces full-duplex operation

Default Configuration

The interface is set to full duplex.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

When configuring a particular duplex mode on the port operating at 10/100 Mbps, disable the auto-negotiation on that port.

Half duplex mode can be set only for ports operating at 10 Mbps or 100 Mbps.

Example

The following example configures the duplex operation of Ethernet port 1 to full duplex operation.

```
Console(config)# interface ethernet 1
Console(config-if)# duplex full
```

negotiation

The **negotiation** Interface Configuration (Ethernet, port-channel) mode command enables auto-negotiation operation for the speed and duplex parameters of a given interface. Use the **no** form of this command to disable auto-negotiation.

NOTE (SPS224G4 combo ports) This command applies when the copper port is used. The configuration does not apply when an SFP is plugged to the port.

Syntax

negotiation [*capability1* [*capability2*...*capability5*]]

no negotiation

Parameters

- *capability* — Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h,100f, 1000f)

Default Configuration

Auto-negotiation is enabled.

If unspecified, the default setting is to enable all capabilities of the port.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

If the capabilities are specified at the time when auto-negotiation is entered, not specifying capabilities when entering auto-negotiation overrides the previous configuration and enables all capabilities.

Example

The following example enables auto-negotiation on Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# negotiation
```

port jumbo-frame

Use port jumbo-frame command to enable jumbo frames for the device. To disable it, use the no form of this command.

Syntax

port jumbo-frame

no port jumbo-frame

Parameters

This command has no arguments or keywords.

Default Configuration

Off

User Guidelines

The command would be effective only after reset.

Command Mode

Global configuration

Examples

```
Console(config)# port jumbo-frame
```

show system flowcontrol

The command is for SPS2024 only.

Use the show system flowcontrol command to display the cascade ports flowcontrol state.

Syntax

show system flowcontrol

Parameters

This command has no arguments or keywords.

Default Configuration

The command has no default configuration.

Command Mode

EXEC

flowcontrol

The **flowcontrol** Interface Configuration (Ethernet, port-channel) mode command configures flow control on a given interface. Use the **no** form of this command to disable flow control.

Syntax

flowcontrol {**auto** | **on** | **off** | **rx** | **tx** }

no flowcontrol

Parameters

- **auto** — Indicates auto-negotiation
- **on** — Enables flow control
- **off** — Disables flow control
- **rx** — Enables receiving pause frames only
- **tx** — Enables transmitting pause frames only

Default Configuration

Flow control is off.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

Negotiation should be enabled for **flow control auto**.

Example

In the following example, flow control is enabled on port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# flowcontrol on
```

mdix

The **mdix** Interface Configuration (Ethernet) mode command enables cable crossover on a given interface. Use the **no** form of this command to disable cable crossover.

NOTE (SPS224G4 combo ports) This command applies when the copper port is used. The configuration does not apply when an SFP is plugged to the port.

Syntax

mdix {**on** | **auto**}

no mdix

Parameters

- **on** — Manual mdix is enabled.
- **auto** — Automatic mdi/mdix is enabled.

Default Configuration

The default setting is **auto**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Auto: All possibilities to connect a PC with cross or normal cables are supported and are automatically detected.

On: It is possible to connect to a PC only with a normal cable and to connect to another device only with a cross cable.

No: It is possible to connect to a PC only with a cross cable and to connect to another device only with a normal cable.

Example

In the following example, automatic crossover is enabled on port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# mdix auto
```

back-pressure

The **back-pressure** Interface Configuration (Ethernet, port-channel) mode command enables back pressure on a given interface. Use the **no** form of this command to disable back pressure.

NOTE (SPS224G4 combo ports) This command applies when the copper port is used. The configuration does not apply when an SFP is plugged to the port.

Syntax

back-pressure

no back-pressure

Default Configuration

Back pressure is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

In the following example back pressure is enabled on port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# back-pressure
```

port jumbo-frame

Use port jumbo-frame command to enable jumbo frames for the device. To disable it, use the no form of this command.

Syntax

port jumbo-frame

no port jumbo-frame

Parameters

This command has no arguments or keywords.

Default Configuration

Off

Usage Guidelines

The command would be effective only after reset.

sfp speed

The **sfp speed** Interface Configuration (Ethernet) mode command configures the speed of an SFP Ethernet interface. Use the **no** form of this command to disable sfp speed.

NOTE The **sfp speed** command is supported in SPS2xx products.

Syntax

sfp speed {**100** | **1000** | **auto**}

no sfp speed

Parameters

- **100** — 100 Mbps
- **1000** — 1000 Mbps
- **auto** — Detects the SFP capabilities, and determines the speed as follows: When multi speed SFP is supported, the highest speed is selected. If SFP capability cannot be detected, 1000 Mbps is selected.

Default Configuration

The default configuration is auto.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the speed at 100 Mbps.

```
Console(config)# interface ethernet 1
Console(config)# sfp speed  100 1
```

clear counters

The **clear counters** Privileged EXEC mode command clears statistics on an interface.

Syntax

clear counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

In the following example, the counters for interface 1 are cleared.

```
Console# clear counters ethernet e1
```

set interface active

The **set interface active** Privileged EXEC mode command reactivates a shutdown interface.

Syntax

set interface active {**ethernet** *interface* | **port-channel** *port-channel-number*}

Parameters

- *interface* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command is used to activate interfaces that were configured to be active, but were shutdown by the system for some reason (e.g., **port security**).

Example

The following example reactivates interface 1.

```
Console# set interface active ethernet 1
```

show interfaces configuration

The **show interfaces configuration** Privileged EXEC mode command displays the configuration for all configured interfaces.

Syntax

show interfaces configuration [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of all configured interfaces:

```
Console# show interfaces configuration

Port  Type       Duplex Speed Neg     Flow Admin Back     Mdix

                                      Ctrl State Pressure Mode
---- ---------- ------ ----- ------- ---- ----- -------- ----
1     100M-Copper Full  100   Enabled Off  Up    Disabled Auto
2     100M-Copper Full  100   Enabled Off  Up    Disabled Auto
3     100M-Copper Full  100   Enabled Off  Up    Disabled Auto
4     100M-Copper Full  100   Enabled Off  Up    Disabled Auto
5     100M-Copper Full  100   Enabled Off  Up    Disabled Auto
6     100M-Copper Full  100   Enabled Off  Up    Disabled Auto
7     100M-Copper Full  100   Enabled Off  Up    Disabled Auto
8     100M-Copper Full  100   Enabled Off  Up    Disabled Auto
9     100M-Copper Full  100   Enabled Off  Up    Disabled Auto
10    100M-Copper Full  100   Enabled Off  Up    Disabled Auto
11    100M-Copper Full  100   Enabled Off  Up    Disabled Auto
```

show interfaces status

The **show interfaces status** Privileged EXEC mode command displays the status of all configured interfaces.

Syntax

show interfaces status [**ethernet** *interface*| **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the status of all configured interfaces.

```
Console# show interfaces status

Port Type       Duplex Speed  Neg    Flow Link  Back     Mdix

                                     Ctrl State Pressure Mode

---- ----------  -----------  ----------- ----- -------- ----
1    100M-Copper --    --    --      --   Down  --       --
2    100M-Copper --    --    --      --   Down  --       --
3    100M-Copper --    --    --      --   Down  --       --
4    100M-Copper --    --    --      --   Down  --       --
5    100M-Copper Full  100   Enabled --   Up    Disabled Auto
6    100M-Copper --    --    --      --   Down  --       --
7    100M-Copper --    --    --      --   Down  --       --
8    100M-Copper --    --    --      --   Down  --       --
9    100M-Copper --    --    --      --   Down  --       --
10   100M-Copper --    --    --      --   Down  --       --
11   100M-Copper --    --    --      --   Down  --       --
12   100M-Copper --    --    --      --   Down  --       --
```

show interfaces advertise

The **show interfaces advertise** Privileged EXEC mode command displays auto-negotiation data.

Syntax

show interfaces advertise [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays auto-negotiation information.

```
Console# show interfaces advertise

Port  Type         Neg      Operational Link Advertisement
----  -----------  -------  ------------------------------
1     100M-Copper  Enabled  --
2     100M-Copper  Enabled  --
3     100M-Copper  Enabled  --
4     100M-Copper  Enabled  --
```

```
5     100M-Copper  Enabled   100f, 100h, 10f, 10h
6     100M-Copper  Enabled   --
7     100M-Copper  Enabled   --
8     100M-Copper  Enabled   --
9     100M-Copper  Enabled   --
10    100M-Copper  Enabled   --
11    100M-Copper  Enabled   --
12    100M-Copper  Enabled   --
```

show interfaces description

The **show interfaces description** Privileged EXEC mode command displays the description for all configured interfaces.

Syntax

show interfaces description [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays descriptions of configured interfaces.

```
Console# show interfaces description

Port     Description
----     -----------
e1       lab
e2
e3
e4
e5
e6
ch1
ch2
```

show interfaces counters

The **show interfaces counters** Privileged EXEC mode command displays traffic seen by the physical interface.

Syntax

show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays traffic seen by the physical interface.

```
Console# show interfaces counters


Port  InOctets  InUcastPkts InMcastPkts  InMcastPkts

---   --------  ----------- -----------  -----------

e1    183892    0           0            0
e2    0         0           0            0
e3    123899    0           0            0


Port  OutOctets OutUcastPkts  OutMcastPkts  OutBcastPkts
---   --------  -----------   -----------   -----------
e1    9188      0             0             0
e2    0         0             0             0
e3    8789      0             0             0


Ch    InOctets  InUcastPkts   InMcastPkts   InMcastPkts
---   --------  -----------   -----------   -----------
1     27889     0             0             0


Ch    OutOctets OutUcastPkts OutMcastPkts  OutBcastPkts
---   --------- ------------ ------------  ------------
1               23739                      0         00
```

The following example displays counters for Ethernet port e1.

```
Console# show interfaces counters ethernet e1

Port  InOctets  InUcastPkts   InMcastPkts   InMcastPkts
---------------------------   -----------   -----------
e1    183892    0             0                   0

Port  OutOctets OutUcastPkts  OutMcastPkts  OutBcastPkts
---------------------------   ------------  ------------
e1    9188      0             0                   0
FCS Errors0
Single Collision Frames0
Late Collisions0
Oversize Packets0
Internal MAC Rx Errors0
Received Pause Frames0
Transmitted Pause Frames0
```

The following table describes the fields shown in the display.

Field	Description
InOctets	Counted received octets.
InUcastPkts	Counted received Unicast packets.
InMcastPkts	Counted received Multicast packets.
InBcastPkts	Counted received Broadcast packets.
OutOctets	Counted transmitted octets.
OutUcastPkts	Counted transmitted Unicast packets.
OutMcastPkts	Counted transmitted Multicast packets.
OutBcastPkts	Counted transmitted Broadcast packets.
FCS Errors	Counted received frames that are an integral number of octets in length but do not pass the FCS check.

Field	Description
Single Collision Frames	Counted frames that are involved in a single collision, and are subsequently transmitted successfully.
Late Collisions	Number of times that a collision is detected later than one slotTime into the transmission of a packet.
Oversize Packets	Counted frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	Counted frames for which reception fails due to an internal MAC sublayer received error.
Received Pause Frames	Counted MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Counted MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

show ports jumbo-frame

The **show ports jumbo**-frame Privileged EXEC mode command displays the configuration of jumbo frames.

Syntax

show ports jumbo-frame

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of jumbo frames on the device.

```
Console# show port jumbo-frame
Jumbo frames are disabled
Jumbo frames will be enabled after reset
```

port storm-control broadcast enable

The **port storm-control broadcast enable** Interface Configuration (Ethernet) mode command enables Broadcast storm control. Use the **no** form of this command to disable Broadcast storm control.

Syntax

port storm-control broadcast enable

no port storm-control broadcast enable

Default Configuration

Broadcast storm control is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Use the **port storm-control broadcast rate** Interface Configuration (Ethernet) mode command, to set the maximum allowable Broadcast rate.

Use the **port storm-control include-multicast** Global Configuration mode command to enable counting Multicast packets in the storm control calculation.

Example

The following example enables Broadcast storm control on port 1 of a device.

```
Console(config)# interface ethernet 1
Console(config-if)# port storm-control broadcast enable
```

port storm-control broadcast rate

The **port storm-control broadcast rate** Interface Configuration (Ethernet) mode command configures the maximum Broadcast rate. Use the **no** form of this command to restore the default configuration.

Syntax

port storm-control broadcast rate *rate*

no port storm-control broadcast rate

Parameters

- *rate* — Maximum kilobits per second of Broadcast and Multicast traffic on a port. (Range for GE ports: 3500 K–100 M,
range for FE ports: 70 K – 100 M, range for SPS2024 devices: 3.5 M - 1 G)

Default Configuration

The default storm control broadcast rate for FE ports is **100 Kbits/Sec** and for GE ports is **500 Kbits/Sec**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Use the **port storm-control broadcast enable** Interface Configuration mode command to enable Broadcast storm control.

Example

The following example configures a port storm-control Broadcast rate of 4000 on port e2.

```
Console(config)# interface ethernet e2
Console(config-if)# port storm-control broadcast rate 4000
```

port storm-control include-multicast

The **port storm-control include-multicast** Interface Configuration mode command enables counting Multicast packets in the **port storm-control broadcast rate** command. Use the **no** form of this command to disable counting Multicast packets.

Syntax

port storm-control include-multicast

no port storm-control include-multicast

Default Configuration

Multicast packets are disabled.

Command Mode

Interface Configuration mode

User Guidelines

To control Multicasts storms, use the **port storm-control broadcast enable** and **port storm-control broadcast rate** commands.

Example

The following example enables counting Multicast packets in the **port storm-control broadcast rate** command.

```
Console(config)# port storm-control include-multicast
```

port storm-control unknown-unicast fastethernet enable

The **port storm-control unknown-unicast fastethernet enable** Global Configuration mode Command enables unknown unicast storm control for FE ports. Use the **no** form of this command to disable storm control.

Syntax

port storm-control unknown-unicast fastethernet enable

no port storm-control unknown-unicast fastethernet enable

Default Configuration

Unknown unicast storm control for FE ports are disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **port storm-control unknown-unicast fastethernet rate** Global Configuration mode command to the set the maximum rate.

The control for GE ports is per port and described in the port storm-control include-multicast interface configuration command.

Example

The following example enables unknown unicast storm control for FE ports.

```
Console(config)# port storm-control unknown-unicast
fastethernet enable
```

port storm-control unknown-unicast fastethernet rate

The **port storm-control unknown-unicast fastethernet rate** Global Configuration mode command configures the maximum rate of unknown unicast storm control for FE ports. Use the **no** form of this command to return to default.

Syntax

port storm-control unknown-unicast fastethernet rate *rate*

no port storm-control unknown-unicast fastethernet rate

Parameters

- *rate* — Maximum of kilobits per second of broadcast traffic on a port. (Range 3.5M - 100M)

Default Configuration

The rate is 3.5M.

Command Mode

Global Configuration mode

User Guidelines

Use the **port storm-control unknown-unicast fastethernet enable** Global Configuration mode command to enable unknown-unicast storm control for FE ports.

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

Example

The following example configures the maximum rate of unknown unicast storm control for FE ports to 10M.

```
console(config)# port storm-control unknown-unicast
fastethernet rate 3500
```

show ports storm-control

The **show ports storm-control** Privileged EXEC mode command displays the storm control configuration.

Syntax

show ports storm-control [*interface*]

Parameters

- *interface* — A valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the storm control configuration.

```
Console# show ports storm-control

Port     State         Rate [Kbits/Sec]     Included
----     -----         ----------------     --------
e1       Disabled      3500                 Broadcast
e2       Disabled      3500                 Broadcast
e3       Disabled      3500                 Broadcast
e4       Disabled      3500                 Broadcast
e5       Disabled      3500                 Broadcast
e6       Disabled      3500                 Broadcast
```

13

GVRP Commands

gvrp enable (Global)

GARP VLAN Registration Protocol (GVRP) is an industry-standard protocol designed to propagate VLAN information from device to device. With GVRP, a single device is manually configured with all desired VLANs for the network, and all other devices on the network learn these VLANs dynamically.

The **gvrp enable** Global Configuration mode command enables GVRP globally. Use the **no** form of this command to disable GVRP on the device.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables GVRP globally on the device.

```
Console(config)# gvrp enable
```

gvrp enable (Interface)

The **gvrp enable** Interface Configuration (Ethernet, port-channel) mode command enables GVRP on an interface. Use the **no** form of this command to disable GVRP on an interface.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is disabled on all interfaces.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

An access port does not dynamically join a VLAN because it is always a member in only one VLAN.

Membership in an untagged VLAN is propagated in the same way as in a tagged VLAN. That is, the PVID is manually defined as the untagged VLAN VID.

Example

The following example enables GVRP on Ethernet port e6.

```
Console(config)# interface ethernet e6
Console(config-if)# gvrp enable
```

garp timer

The **garp timer** Interface Configuration (Ethernet, Port channel) mode command adjusts the values of the join, leave and leaveall timers of GARP applications. Use the **no** form of this command to restore the default configuration.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*

no garp timer

Parameters

- {**join** | **leave** | **leaveall**} — Indicates the type of timer.
- *timer_value* — Timer values in milliseconds in multiples of 10. (Range: 10-2147483640)

Default Configuration

Following are the default timer values:

- Join timer — 200 milliseconds
- Leave timer — 600 milliseconds
- Leaveall timer — 10000 milliseconds

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The following relationship must be maintained between the timers:

Leave time must be greater than or equal to three times the join time.

Leave-all time must be greater than the leave time.

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on Layer 2-connected devices, the GARP application will not operate successfully.

Example

The following example sets the leave timer for Ethernet port e6 to 900 milliseconds.

```
Console(config)# interface ethernet e6
Console(config-if)# garp timer leave 900
```

gvrp vlan-creation-forbid

The **gvrp vlan-creation-forbid** Interface Configuration (Ethernet, port-channel) mode command disables dynamic VLAN creation or modification. Use the **no** form of this command to enable dynamic VLAN creation or modification.

Syntax

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Default Configuration

Dynamic VLAN creation or modification is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command forbids dynamic VLAN creation from the interface. The creation or modification of dynamic VLAN registration entries as a result of the GVRP exchanges on an interface are restricted only to those VLANs for which static VLAN registration exists.

Example

The following example disables dynamic VLAN creation on Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# gvrp vlan-creation-forbid
```

gvrp registration-forbid

The **gvrp registration-forbid** Interface Configuration (Ethernet, port-channel) mode command de-registers all dynamic VLANs on a port and prevents VLAN creation or registration on the port. Use the **no** form of this command to allow dynamic registration of VLANs on a port.

Syntax

gvrp registration-forbid

no gvrp registration-forbid

Default Configuration

Dynamic registration of VLANs on the port is allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example forbids dynamic registration of VLANs on Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# gvrp registration-forbid
```

clear gvrp statistics

The **clear gvrp statistics** Privileged EXEC mode command clears all GVRP statistical information.

Syntax

clear gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears all GVRP statistical information on Ethernet port 1.

```
Console# clear gvrp statistics ethernet 1
```

show gvrp configuration

The **show gvrp configuration** Privileged EXEC mode command displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.

Syntax

show gvrp configuration [**ethernet** *interface* |**port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays GVRP configuration information.

```
Console# show gvrp configuration

GVRP Feature is currently enabled on the device.

                                          Timers (milliseconds)

Port(s) Status  Registration Dynamic VLAN Join Leave Leave All
                             Creation

------  ------  ------------ ------------ ---- ----- ---------

e1      Enabled Normal       Enabled      200  600   10000
e4      Enabled Normal       Enabled      200  600   10000
```

show gvrp statistics

The **show gvrp statistics** Privileged EXEC mode command displays GVRP statistics.

Syntax

show gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows GVRP statistical information.

```
Console# show gvrp statistics

GVRP Statistics:
Legend:
rJE :     Join Empty Received      rJIn :     Join In Received
rEmp:     Empty Received           rLIn :    Leave In Received
rLE :     Leave Empty Received     rLA  :   Leave All Received
sJE :     Join Empty Sent          sJIn :     Join In Sent
sEmp:     Empty Sent               sLIn :     Leave In Sent
sLE :     Leave Empty Sent         sLA  :     Leave All Sent
Port rJE  rJIn  rEmp  rLIn  rLE  rLA  sJE  sJIn  sEmp sLIn sLE sLA
```

show gvrp error-statistics

The **show gvrp error-statistics** Privileged EXEC mode command displays GVRP error statistics.

Syntax

show gvrp error-statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays GVRP statistical information.

```
Console# show gvrp error-statistics

GVRP Error Statistics

Legend:
INVPROT :  Invalid Protocol Id      INVALEN : Invalid Attribute Length
INVATYP :  Invalid Attribute Type   INVEVENT: Invalid Event
INVAVAL :  Invalid Attribute Value
 Port INVPROT INVATYP INVAVAL INVALEN INVEVENT
```

IGMP Snooping Commands

ip igmp snooping (global)

The **ip igmp snooping** Global Configuration mode command enables Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable IGMP snooping.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping can only be enabled on static VLANs. It must not be enabled on Private VLANs or their community VLANs.

Example

The following example enables IGMP snooping.

```
Console(config)# ip igmp snooping
```

ip igmp snooping (Interface)

The **ip igmp snooping** Interface Configuration (VLAN) mode command enables Internet Group Management Protocol (IGMP) snooping on a specific VLAN. Use the **no** form of this command to disable IGMP snooping on a VLAN interface.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

IGMP snooping can only be enabled on static VLANs. It must not be enabled on Private VLANs or their community VLANs.

Example

The following example enables IGMP snooping on VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping
```

ip igmp snooping mrouter

The **ip igmp snooping mrouter** Interface Configuration (VLAN) mode command enables automatic learning of Multicast device ports in the context of a specific VLAN. Use the **no** form of this command to remove automatic learning of Multicast device ports.

Syntax

ip igmp snooping mrouter learn-pim-dvmrp

no ip igmp snooping mrouter learn-pim-dvmrp

Default Configuration

Automatic learning of Multicast device ports is enabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Multicast device ports can be configured statically using the **bridge multicast forward-all** Interface Configuration (VLAN) mode command.

Example

The following example enables automatic learning of Multicast device ports on VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping mrouter learn-pim-dvmrp
```

ip igmp snooping querier enable

Use the **ip igmp snooping querier enable** interface configuration command to enable Internet Group Management Protocol (IGMP) querier on a specific VLAN. Use the **no** form of this command to disable IGMP querier on a VLAN interface.

Syntax

ip igmp snooping querier enable

no ip igmp snooping querier enable

Default Configuration

Disabled

Command Mode

Interface configuration mode (VLAN)

User Guidelines

- IGMP snooping querier can be enabled on a VLAN only if IGMP snooping is enabled for that VLAN.
- No more then one switch can be configured as an IGMP Querier for a VLAN.
- When IGMP Snooping Querier is enabled, it starts after host-time-out/2 with no IGMP traffic detected from a multicast router.
- The IGMP Snooping Querier would disable itself if it detects IGMP traffic from a multicast router. It would restart itself after host-time-out/2.
- Following are the IGMP Snooping Querier parameters as function of the IGMP Snooping parameters:
  - QueryMaxResponseTime: host-time-out/10
  - QueryInterval: host-time-out/3

ip igmp snooping host-time-out

The **ip igmp snooping host-time-out** Interface Configuration (VLAN) mode command configures the host-time-out. If an IGMP report for a Multicast group is not received for a host-time-out period from a specific port, this port is deleted from the member list of that Multicast group. Use the **no** form of this command to restore the default configuration.

Syntax

ip igmp snooping host-time-out *time-out*

no ip igmp snooping host-time-out

Parameters

- *time-out* — Specifies the host timeout in seconds. (Range: 60 - 2147483647)

Default Configuration

The default host-time-out is **260** seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The timeout should be at least greater than 2*query_interval+max_response_time of the IGMP router.

Example

The following example configures the host timeout to 300 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping host-time-out 300
```

ip igmp snooping mrouter-time-out

The **ip igmp snooping mrouter-time-out** Interface Configuration (VLAN) mode command configures the mrouter-time-out. The ip igmp snooping mrouter-time-out Interface Configuration (VLAN) mode command is used for setting the aging-out time after Multicast device ports are automatically learned. Use the **no** form of this command to restore the default configuration.

Syntax

ip igmp snooping mrouter-time-out *time-out*

no ip igmp snooping mrouter-time-out

Parameters

- *time-out* — Specifies the host timeout in seconds. (Range: 60 - 2147483647)

Default Configuration

The default host-time-out is **300** seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Mrouter port is aged out between time-out to time-out*2 seconds after the last Multicast router traffic on the port.

Example

The following example configures the Multicast device timeout to 200 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping mrouter-time-out 200
```

ip igmp snooping leave-time-out

The **ip igmp snooping leave-time-out** Interface Configuration (VLAN) mode command configures the leave-time-out. If an IGMP report for a Multicast group is not received for a leave-time-out period after an IGMP Leave is received from one of the ports in the VLAN, this port is deleted from the member list of that Multicast group. Use the **no** form of this command to restore the default configuration.

Syntax

ip igmp snooping leave-time-out {*time-out* | **immediate-leave**}

no ip igmp snooping leave-time-out

Parameters

- *time-out* — Specifies the leave-timeout in seconds for IGMP queries. (Range: 0-2147483647)
- **immediate-leave** — Indicates that the port should be immediately removed from the members list after receiving IGMP Leave.

Default Configuration

The default leave-time-out configuration is **10** seconds.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

The leave timeout should be set greater than the maximum time that a host is allowed to respond to an IGMP query.

Use immediate leave only where there is just one host connected to a port.

Example

The following example configures the host leave timeout to 60 seconds.

```
Console(config)# interface vlan 2
Console(config-if)# ip igmp snooping leave-time-out 60
```

ip igmp snooping multicast-tv

The **ip igmp snooping multicast-tv** Global Configuration mode command defines the Multicast ip-addresses that are associated with a Multicast-TV VLAN. Use the **no** form of this command to remove all associations.

Syntax

ip igmp snooping multicast-tv vlan *vlan-id* {**add** | **remove**} *ip-multicast-address* [**count** *number*]

no ip igmp snooping multicast-tv vlan *vlan-id*

Parameters

- *vlan-id* — Specifies the VLAN ID of the Multicast-TV VLAN.
- *ip-multicast-address* — Specifies an IP address to associate with the Multicast-TV VLAN.
- *number* — Configures multiple contiguous Multicast IP addresses. If unspecified, the default is 1. (Range: 1-256)

Default Configuration

The default configuration has **no** Multicast IP address associated with it.

Command Mode

Global Configuration mode

User Guidelines

Use this command to define the Multicast transmissions on a Multicast-TV VLAN. The configuration is only relevant for an access port, which is a member in the configured VLAN as a Multicast-TV VLAN. If an IGMP message is received on such an access port, it is associated with the Multicast-TV VLAN provided that one of the Multicast IP addresses are associated with the Multicast-TV VLAN.

Bridge Multicast filtering should be enabled prior to configuring this command.

Example

The following example defines the Multicast ip-addresses that are associated with a Multicast-tv VLAN. Use the **no** form of this command to remove all associations.

```
Console (config)# ip igmp snooping multicast-tv vlan 100 add
239.255.0.0 256
```

ip igmp snooping map cpe vlan

The **ip igmp snooping map cpe vlan** Global Configuration mode command maps CPE VLANs to Multicast-TV VLANs. Use the **no** form of this command to remove the mapping.

Syntax

ip igmp snooping map cpe vlan *vlan-id* **multicast-tv vlan** *vlan-id*

no ip igmp snooping map cpe vlan *vlan-id*

Parameters

- **cpe vlan** *vlan-id* — Specifies the CPE VLAN.
- **multicast-tv vlan** *vlan-id* —Specifies the Multicast VLAN.

Default Configuration

No mapping exists.

Command Mode

Global configuration

Command Usage

Use this command to associate CPE VLAN to a Multicast-TV VLAN.

If an IGMP message is received on a customer port tagged with a CPE VLAN, and there is a mapping from that CPE VLAN to a Multicast-TV VLAN, the IGMP message is associated with the Multicast-TV VLAN.

Example

The following example maps an internal CPE VLAN number 4 to the Multicast TV VLAN number 300.

```
Console (config)# ip igmp snooping map cpe vlan 4 multicast-tv
vlan 300
```

show ip igmp snooping mrouter

The **show ip igmp snooping mrouter** Privileged EXEC mode command displays information on dynamically learned Multicast device interfaces.

Syntax

show ip igmp snooping mrouter [**interface** *vlan-id*]

Parameters

- *vlan-id* — Specifies the VLAN number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays Multicast device interfaces in VLAN 1000.

```
Console# show ip igmp snooping mrouter interface 1000

VLAN                          Ports
----                          -----
1000                          e1

Detected Multicast devices that are forbidden statically:
VLAN                          Ports
----                          -----
1000                          19
```

show ip igmp snooping interface

The **show ip igmp snooping interface** Privileged EXEC mode command displays IGMP snooping configuration.

Syntax

show ip igmp snooping interface *vlan-id*

Parameters

- *vlan-id* — Specifies the VLAN number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays IGMP snooping information on VLAN 1000.

```
Console # show ip igmp snooping interface 1000

IGMP Snooping is globally enabled

IIGMP snooping is enabled on VLAN 1000

IGMP snooping querier admin: Enabled
IGMP snooping querier oper: Enabled

IGMP host timeout is 300 sec
IGMP Immediate leave is disabled
IGMP leave timeout is 10 sec
IGMP mrouter timeout is 300 sec
```

show ip igmp snooping groups

The **show ip igmp snooping groups** Privileged EXEC mode command displays Multicast groups learned by IGMP snooping.

Syntax

show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*]

Parameters

- *vlan-id* — Specifies the VLAN number
- *ip-multicast-address* — Specifies the IP Multicast address

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

To see the full Multicast Address Table (including static addresses) use the **show bridge multicast address-table** Privileged EXEC command.

Example

The following example shows IGMP snooping information on Multicast groups.

```
Console# show ip igmp snooping groups

Vlan     Group            Source               Include
         Address          Address              Ports

1        231.2.2.3        172.16.1.1           e1

1        231.2.2.3        172.16.1.2           e2

19       231.2.2.8        172.16.1.1           e9

19       231.2.2.8        172.16.1.2           e10-e11

IGMP Reporters that are forbidden statically:

Vlan      Group Address   Source address       Ports

----      -------------   --------------       --------

1         231.2.2.3       172.16.1.1           e8

19        231.2.2.8       172.16.1.1           e8
```

show ip igmp snooping multicast-tv

The **show ip igmp snooping multicast-tv** Privileged EXEC mode command displays the IP addresses associated with Multicast TV VLANs.

Syntax

show ip igmp snooping multicast-tv [**vlan** *vlan-id*]

Parameters

- *vlan-id* — Specifies the VLAN ID value.
- *ip-multicast-address* — Specifies the IP Multicast address.

Default Configuration

This command has **no** default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

No user guidelines for this command.

Example

The following example displays the IP addresses associated with Multicast TV VLANs.

```
Console # show ip igmp snooping multicast-tv

VLAN                           IP address
------                         -------------
1000                           239.255.0.1
1000                           239.255.0.2
1000                           239.255.0.3
```

```
1000                          239.255.0.4
1000                          239.255.0.5
1000                          239.255.0.6
1000                          239.255.0.7
1000                          239.255.0.0
```

show ip igmp snooping cpe vlans

The **show ip igmp snooping cpe vlans** Privileged EXEC mode command displays the CPE VLANs to Multicast TV VLANs mappings.

Syntax

show ip igmp snooping cpe vlans [**vlan** *vlan-id*]

Parameters

- *vlan-id* — CPE VLAN ID value.

Default Configuration

This command has **no** default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

No user guidelines for this command.

Example

The following example displays the CPE VLANs to Multicast TV VLAN mappings.

```
Console # show ip igmp snooping cpe vlans

CPE VLAN                 Multicast-TV VLAN
--------                 -------------
2                        1118
3                        1119
```

15

IP Address Commands

ip address

The **ip address** Interface Configuration (VLAN) mode command sets an IP address. Use the **no** form of this command to remove an IP address.

Syntax

ip address *ip-address* {*mask* | *prefix-length*} [**default-gateway** *ip-address*]

no ip address [*ip-address*]

Parameters

- *ip-address* — Specifies the valid IP address
- *mask* — Specifies the valid network mask of the IP address.
- *prefix-length* — Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 8-30)
- **default-gateway** *ip-address*—Specifies the IP address of the default gateway.

Default Configuration

No IP address is defined for interfaces.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

An IP address cannot be configured for a range of interfaces (range context).

This command is only functional if the device is in Switch mode.

Example

The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console(config)# interface vlan 1
Console(config-if)# ip address 131.108.1.27 255.255.255.0
```

ip address dhcp

The **ip address dhcp** Interface Configuration (VLAN) mode command acquires an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. Use the **no** form of this command to de-configure an acquired IP address.

Syntax

ip address dhcp [**hostname** *host-name*]

no ip address dhcp

Parameters

- *host-name* — Specifies the name of the host to be placed in the DHCP option 12 field. This name does not have to be the same as the host name specified in the **hostname** Global Configuration mode command. (Range: 1-20 characters)

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command is only functional if the device is in Switch mode.

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol.

Some DHCP servers require that the DHCPDISCOVER message have a specific host name. The **ip address dhcp hostname** *host-name* command is most typically used when the host name is provided by the system administrator.

If the device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If the **ip address dhcp** command is used with or without the optional keyword, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the specified DHCP host name is the globally configured host name of the device. However, the **ip address dhcp hostname** *host-name* command can be used to place a different host name in the DHCP option 12 field.

The **no ip address dhcp** command de-configures any IP address acquired, and sends a DHCPRELEASE message.

Example

The following example acquires an IP address for Ethernet port e16 from DHCP.

```
Console(config)# interface vlan 1
Console(config-if)# ip address dhcp
```

renew dhcp

The **renew dhcp** Privileged EXEC mode command renews an IP address acquired from a DHCP server.

Syntax

renew dhcp [force-autoconfig]

Parameters

- **force-autoconfig** — If the DHCP server holds a DHCP option 67 record for the assigned IP address, the file would overwrite the existing device configuration

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Please note that this command does not enable DHCP. If DHCP is not enabled, the command returns an error message.

If an IP address is already acquired, the command tries to renew that IP address.

If an IP address isn’t acquired yet, the command initiates a DHCP request.

Example

The following example renews an IP address acquired from a DHCP server for specific interface.

```
Console# renew dhcp
```

ip default-gateway

The **ip default-gateway** Global Configuration mode command defines a default gateway (device). Use the **no** form of this command to restore the default configuration.

Syntax

ip default-gateway *ip-address*

no ip default-gateway

Parameters

- *ip-address* — Specifies the valid IP address of the currently defined default gateway.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

This command is only operational in Switch mode.

Example

The following example defines default gateway 192.168.1.1.

```
Console(config)# ip default-gateway 192.168.1.1
```

show ip interface

The **show ip interface** Privileged EXEC mode command displays the usability status of configured IP interfaces.

Syntax

show ip interface [**vlan** *vlan-id*]

Parameters

- *vlan-id* — Specifies a valid VLAN number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example the displays the configured IP interfaces and their types.

```
Console# show ip interface

Proxy ARP is disabled

IP addressI/F                 Type     Direct Broadcast
-----------                   -------  ----------------
10.7.1.192/241                Static   disable
10.7.2.192/242                Static   disable
```

arp

The **arp** Global Configuration mode command adds a permanent entry in the Address Resolution Protocol (ARP) cache. Use the **no** form of this command to remove an entry from the ARP cache.

Syntax

arp *ip_addr hw_addr* {**vlan** *vlan-id*}

no arp *ip_addr* {**vlan** *vlan-id*}

Parameters

- *ip_addr* — Valid IP address or IP alias to map to the specified MAC address.
- *hw_addr* — Valid MAC address to map to the specified IP address or IP alias.
- *vlan-id* — Valid VLAN number.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses. Because most hosts support dynamic resolution, static ARP cache entries do not generally have to be specified.

Example

The following example adds IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
Console(config)# arp 198.133.219.232 00:00:0c:40:0f:bc
```

arp timeout

The **arp timeout** Global Configuration mode command configures how long an entry remains in the ARP cache. Use the **no** form of this command to restore the default configuration.

Syntax

arp timeout *seconds*

no arp timeout

Parameters

- *seconds* — Time (in seconds) that an entry remains in the ARP cache. (Range: 1-40000000)

Default Configuration

The default timeout is **60000** seconds.

Command Mode

Global Configuration mode

User Guidelines

It is recommended not to set the timeout value to less than 3600.

Example

The following example configures the ARP timeout to 12000 seconds.

```
Console(config)# arp timeout 12000
```

clear arp-cache

The **clear arp-cache** Privileged EXEC mode command deletes all dynamic entries from the ARP cache.

Syntax

clear arp-cache

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```

show arp

The **show arp** Privileged EXEC mode command displays entries in the ARP table.

Syntax

show arp [ip-address *ip-address*] [**mac-address** *mac-address*]

Parameters

- *ip-address* — Displays the ARP entry of a specific IP address
- *mac-address* — Displays the ARP entry of a specific MAC address

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

When an ARP entry is associated with an IP interface defined on a port or port-channel, the VLAN field is empty.

Example

The following example displays entries in the ARP table.

```
Console# show arp

ARP timeout: 80000 Seconds
```

```
VLAN    IP Address                      HW AddressStatus
------  -----------                     ----------------------
VLAN 1  10.7.1.102                      00:10:B5:04:DB:4B
Dynamic
VLAN 1  10.7.1.135                      00:50:22:00:2A:A4Static
```

ip domain-lookup

The **ip domain-lookup** Global Configuration mode command enables the IP Domain Naming System (DNS)-based host name-to-address translation. Use the **no** form of this command to disable DNS-based host name-to-address translation.

Syntax

ip domain-lookup

no ip domain-lookup

Default Configuration

IP Domain Naming System (DNS)-based host name-to-address translation is enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables IP Domain Naming System (DNS)-based host name-to-address translation.

```
Console(config)# ip domain-lookup
```

ip domain-name

The **ip domain-name** Global Configuration mode command defines a default domain name used by the software to complete unqualified host names (names without a dotted-decimal domain name). Use the **no** form of this command to remove the default domain name.

Syntax

ip domain-name *name*

no ip domain-name

Parameters

- *name* — Specifies the default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Range: 1-158 characters)

Default Configuration

A default domain name is not defined.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines default domain name www.LinkSys.com.

```
Console(config)# ip domain-name www.LinkSys.com
```

ip name-server

The **ip name-server** Global Configuration mode command defines the available name servers. Use the **no** form of this command to remove a name server.

Syntax

ip name-server *server-address* [*server-address2* ... *server-address8*]

no ip name-server [*server-address1* ... *server-address8*]

Parameters

- *server-address* — Specifies IP addresses of the name server.

Default Configuration

No name server addresses are specified.

Command Mode

Global Configuration mode

User Guidelines

The preference of the servers is determined by the order in which they were entered.

Up to 8 servers can be defined using one command or using multiple commands.

Example

The following example sets the available name server.

```
Console(config)# ip name-server 176.16.1.18
```

ip host

The **ip host** Global Configuration mode command defines static host name-to-address mapping in the host cache. Use the **no** form of this command to remove the name-to-address mapping.

Syntax

ip host *name address*

no ip host *name*

Parameters

- *name* — Specifies the name of the host. (Range: 1-158 characters)
- *address* — Specifies the associated IP address.

Default Configuration

No host is defined.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines a static host name-to-address mapping in the host cache.

```
Console(config)# ip host accounting.LinkSys.com 176.10.23.1
```

clear host

The **clear host** Privileged EXEC mode command deletes entries from the host name-to-address cache.

Syntax

clear host {*name* | *}

Parameters

- *name* — Specifies the host entry to be removed. (Range: 1-158 characters)
- * — Removes all entries.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example deletes all entries from the host name-to-address cache.

```
Console# clear host *
```

clear host dhcp

The **clear host dhcp** Privileged EXEC mode command deletes entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).

Syntax

clear host dhcp {*name* | *}

Parameters

- *name* — Specifies the host entry to be removed. (Range: 1-158 characters)
- * — Removes all entries.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

This command is only operational in Switch mode.

This command deletes the host name-to-address mapping temporarily until the next renewal of the IP address.

Example

The following example deletes all entries from the host name-to-address mapping.

```
Console# clear host dhcp *
```

show hosts

The **show hosts** Privileged EXEC mode command displays the default domain name, a list of name server hosts, the static and the cached list of host names and addresses.

Syntax

show hosts [*name*]

Parameters

- *name* — Specifies the host name. (Range: 1-158 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays host information.

```
Console# show hosts

System name: Device
Default domain is gm.com, sales.gm.com, usa.sales.gm.com(DHCP)
Name/address lookup is enabled
Name servers (Preference order): 176.16.1.18 176.16.1.19
```

```
Configured host name-to-address mapping:

Host                            Addresses
----                            ---------
accounting.gm.com               176.16.8.8 176.16.8.9 (DHCP)


Cache               TTL(Hours)
Host                Total       Elapsed     Type       Addresses
----                -----       -------     ----       ---------
www.stanford.edu    72          3           IP         171.64.14.203
```

16

IP Source Guard Commands

ip source-guard (global)

The **ip source-guard** Global Configuration mode command globally enables the IP source guard. Use the **no** form of this command to disable IP source guard.

Syntax

ip source-guard

no ip source-guard

Default Configuration

IP source guard is disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables the IP source guard.

```
Console(config)# ip source-guard
```

ip source-guard (interface)

The **ip source-guard** Interface Configuration (Ethernet, Port-channel) mode command enables IP source guard on an interface. Use the **no** form of this command to disable IP source guard.

Syntax

ip source-guard

no ip source-guard

Default Configuration

IP source guard is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

IP source guard must first be globally enabled before enabling IP source guard on an interface.

IP source guard is effective only on DHCP snooping untrusted interface, although it can be enabled (as a shadow configuration) on a trusted interface.

Example

The following example enables IP source guard on an interface.

```
Console(config)# interface ethernet 1
Console(config-if)# ip source-guard
```

ip source-guard binding

The **ip source-guard** binding Global Configuration mode command configures the static IP source bindings on the switch. Use the **no** form of this command to delete static bindings.

Syntax

ip source-guard binding *mac-address vlan-id ip-address* {**ethernet** *interface* | **port-channel** *port-channel-number*}

no ip source-guard binding *mac-address vlan-id*

Parameters

- *mac-address* — Specifies a MAC address.
- *vlan-id* — Specifies a VLAN number.
- *ip-address* — Specifies an IP address.
- *interface* — Specifies an Ethernet port.
- *port-channel-number* — Specifies the Port-channel number.

Default Configuration

No static binding exists.

Command Mode

Global Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the static IP source bindings on the switch.

```
Console(config)# ip source-guard binding 00:01:01:02:02:02 1
192.168.2.10 ethernet e2
```

ip source-guard tcam retries-freq

The **ip source-guard tcam retries-freq** Global Configuration mode command configures the frequency of retries for TCAM resources for inactive IP source guard addresses. Use the **no** form of this command to return to the default configuration.

Syntax

ip source-guard tcam retries-freq {*seconds* | **never**}

no ip source-guard tcam retries-freq

Parameters

- *seconds* — Specifies, in seconds, the retries frequency. (Range: 10 – 600)
- **never** — Specifies to not perform an automatic search for TCAM resources.

Default Configuration

The default value is **60**.

Command Mode

Global Configuration mode.

User Guidelines

Since the IP source guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations where IP source guard addresses are inactive because of a lack of TCAM resources. By default, every minute the software conducts a search for available space in the TCAM for the inactive IP source guard addresses. You can use this command to change the frequency or to disable automatic retries for TCAM space.

The **show ip source-guard inactive** EXEC mode command displays the inactive IP source guard addresses.

Example

The following example configures the frequency of retries for TCAM resources for inactive IP source guard addresses.

```
Console(config)# ip source-guard tcam retries-freq
```

show ip source-guard configuration

The **show ip source-guard configuration** Privileged EXEC mode command displays the IP source guard configuration.

Syntax

show ip source-guard configuration [ethernet *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface*—Specify Ethernet port.
- *port-channel-number*—Specify Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the IP source guard configuration.

```
Console# show ip source-guard configuration

IP source guard is globally enabled

Interface     State
------------  --------------
e21           Enabled
e22           Enabled
e23           Enabled
e24           Enabled
e32           Enabled
e33           Enabled
e34           Enabled
```

show ip source-guard status

The **show ip source-guard status** Privileged EXEC mode command displays the IP source guard status.

Syntax

show ip source-guard status [**mac-address** *mac-address*] [**ip-address** *ip-address*] [**vlan** *vlan-id*] [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *mac-address*—Specifies a MAC address.
- *ip-address*—Specifies an IP address.
- *vlan-id*—Specifies a VLAN number.
- *interface*—Specifies an Ethernet port.
- *port-channel-number*—Specifies a Port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example.

```
Console# show ip source-guard status

IP source guard is globally disabled.

Console# show ip source-guard status

Interface Filter Status   IP Address Mac Address    VLAN Type
--------- ------ ------   ---------  -------------- ---- ------
e21       IP     Active   10.1.8.1   0060.704C.73FF 3    DHCP
e22       IP     Active   10.1.8.2   0060.704C.7BC1 3    DHCP
e23       IP     Active   10.1.12.2  0060.704C.7BC3 4    DHCP
e24       IP     Active   Deny all
e32       IP     Active   10.1.8.218 0060.704C.7BAC 3    Static
e33       IP     Inactive 10.1.8.32  0060.704C.83FF 3    DHCP
e34       IP     Inactive
e35       IP     Inactive
```

show ip source-guard inactive

The **show ip source-guard inactive** Privileged EXEC mode command displays the IP source guard inactive addresses.

Syntax

show ip source-guard inactive

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Since the IP source guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations where IP source guard addresses are inactive because of lack of TCAM resources.

By default, every minute the software conducts a search for available space in the TCAM for the inactive IP source guard addresses.

The **ip source-guard tcam retries-freq** Global Configuration mode command changes the frequency or disables automatic retries for TCAM space.

This command displays the inactive IP source guard addresses.

Example

The following example displays the IP source guard inactive addresses.

```
Console# show ip source-guard inactive

TCAM resources search frequency: 10 minutes
```

```
Interface Filter IP Address MAC Address    VLAN  Type  Reason
--------- ------ ---------- ----------     ----  ----- ------
e32       IP     10.1.8.32  0060.704C.83FF 3     3DHCP Resource
                                                       Problem
```

LACP Commands

lacp system-priority

The **lacp system-priority** Global Configuration mode command configures the system priority. Use the **no** form of this command to restore the default configuration.

Syntax

lacp system-priority *value*

no lacp system-priority

Parameters

- *value* — Specifies system priority value. (Range: 1-65535)

Default Configuration

The default system priority is **1**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the system priority to 120.

```
Console(config)# lacp system-priority 120
```

lacp port-priority

The **lacp port-priority** Interface Configuration (Ethernet) mode command configures physical port priority. Use the **no** form of this command to return to the default configuration.

Syntax

lacp port-priority *value*

no lacp port-priority

Parameters

- *value* — Specifies port priority. (Range: 1-65535)

Default Configuration

The default port priority is **1**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the priority of Ethernet port e6 as 247.

```
Console(config)# interface ethernet e6
Console(config-if)# lacp port-priority 247
```

lacp timeout

The **lacp timeout** Interface Configuration (Ethernet) mode command assigns an administrative LACP timeout. Use the **no** form of this command to return to the default configuration.

Syntax

lacp timeout {**long** | **short**}

no lacp timeout

Parameters

- **long** — Specifies the long timeout value.
- **short** — Specifies the short timeout value.

Default Configuration

The default port timeout value is **long**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example assigns a long administrative LACP timeout to Ethernet port e6.

```
Console(config)# interface ethernet e6
Console(config-if)# lacp timeout long
```

show lacp ethernet

The **show lacp ethernet** Privileged EXEC mode command displays LACP information for Ethernet ports.

Syntax

show lacp ethernet *interface* [**parameters** | **statistics** | **protocol-state**]

Parameters

- *interface* — Valid Ethernet port.
- **parameters** — Link aggregation parameter information.
- **statistics** — Link aggregation statistics information.
- **protocol-state** — Link aggregation protocol-state information.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example display LACP information for Ethernet port e1.

```
Console# show lacp ethernet e1

e1 LACP parameters:
    Actor
        system priority:                    1
        system mac addr:                    00:00:12:34:56:78
        port Admin key:                     30
        port Oper key:                      30
        port Oper number:                   21
        port Admin priority:                1
        port Oper priority:                 1
        port Admin timeout:                 LONG
        port Oper timeout:                  LONG
        LACP Activity:                      ACTIVE
        Aggregation:                        AGGREGATABLE
        synchronization:                    FALSE
        collecting:                         FALSE
        distributing:                       FALSE
        expired:                            FALSE
    Partner
        system priority:                    0
        system mac addr:                    00:00:00:00:00:00
        port Admin key:                     0
        port Oper key:                      0
        port Oper number:                   0
        port Admin priority:                0
        port Oper priority:                 0
        port Oper timeout:                  LONG
        LACP Activity:                      PASSIVE
        Aggregation:                        AGGREGATABLE
        synchronization                     FALSE
        collecting:                         FALSE
        distributing:                       FALSE
        expired:                            FALSE
```

```
e1 LACP Statistics:
ACP PDUs sent:                            2
LACP PDUs received:                       2

e1 LACP Protocol State:
    LACP State Machines:
        Receive FSM:                      Port Disabled State
        Mux FSM:                          Detached State
        Periodic Tx FSM:                  No Periodic State
    Control Variables:
        BEGIN:                            FALSE
        LACP_Enabled:                     TRUE
        Ready_N:                          FALSE
        Selected:                         UNSELECTED
        Port_moved:                       FALSE
        NNT:                              FALSE
        Port_enabled:                     FALSE
    Timer Counters
        periodic tx timer:                0
        current while timer:              0
        wait while timer:                 0
```

show lacp port-channel

The **show lacp port-channel** Privileged EXEC mode command displays LACP information for a port-channel.

Syntax

show lacp port-channel [*port_channel_number*]

Parameters

- *port_channel_number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays LACP information about port-channel 1.

```
Console# show lacp port-channel 1

Port-Channel ch1
    Port Type Gigabit Ethernet
    Attached Lag id:
    Actor
        System Priority:       1
        MAC Address:           00:02:85:0E:1C:00
        Admin Key:             1000
        Oper Key:              1000
    Partner
        System Priority:       0
        MAC Address:           00:00:00:00:00:00
        Oper Key:              14
```

18

Line Commands

line

The **line** Global Configuration mode command identifies a specific line for configuration and enters the Line Configuration command mode.

Syntax

line {**console** | **telnet** | **ssh**}

Parameters

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the device as a virtual terminal for remote console access.

```
Console(config)# line telnet
Console(config-line)#
```

speed

The **speed** Line Configuration mode command sets the line baud rate. Use the no form of this command to restore the default configuration.

Syntax

speed *bps*

no speed

Parameters

- *bps* — Baud rate in bits per second (bps). Possible values are 2400, 4800, 9600, 19200, 38400, 57600 and 115200.

Default Configuration

The default speed is **9600** bps.

Command Mode

Line Configuration (console) mode

User Guidelines

This command is available only on the line console.

This configuration applies only to the current session.

Example

The following example configures the line baud rate.

```
Console(config)# line console
Console(config-line)# speed 115200
```

exec-timeout

The **exec-timeout** Line Configuration mode command sets the interval that the system waits until user input is detected. Use the **no** form of this command to restore the default configuration.

Syntax

exec-timeout *minutes* [*seconds*]

no exec-timeout

Parameters

- *minutes* — Specifies the number of minutes for the timeout. (Range: 0-65535)
- *seconds* — Specifies additional time intervals in seconds. (Range: 0-59)

Default Configuration

The default configuration is 10 minutes.

Command Mode

Line Configuration mode

User Guidelines

To specify no timeout, enter the **exec-timeout 0** command.

Example

The following example configures the interval that the system waits until user input is detected to 20 minutes.

```
Console(config)# line console
Console(config-line)# exec-timeout 20
```

show line

The **show line** Privileged EXEC mode command displays line parameters.

Syntax

show line [**console** | **telnet** | **ssh**]

Parameters

- **console** — Console terminal line.
- **telnet** — Virtual terminal for remote console access (Telnet).
- **ssh** — Virtual terminal for secured remote console access (SSH).

Default Configuration

If the line is not specified, the default value is console.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the line configuration.

```
Console# show line

Console configuration:
        Interactive timeout: Disabled
        History: 10
        Baudrate: 9600
        Databits: 8
        Parity: none
        Stopbits: 1

Telnet configuration:
        Interactive timeout: 10 minutes 10 seconds
        History: 10

SSH configuration:
        Interactive timeout: 10 minutes 10 seconds
        History: 10
```

19

Management ACL Commands

management access-list

The **management access-list** Global Configuration mode command configures a management Access List and enters the Management Access-List Configuration command mode. Use the **no** form of this command to delete an Access List.

Syntax

management access-list *name*

no management access-list *name*

Parameters

- *name*— Specifies the Access List name. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure a management Access List. This command converts the device to Access-List Configuration mode, where the denied or permitted access conditions with the deny and permit commands must be defined.

If no match criteria are defined the default is '**deny**'.

If the device is reentered to an Access-List context, the new rules are entered at the end of the Access-List.

Use the management access-class command to choose the active Access-List.

The active management list cannot be updated or removed.

For IPv6 management traffic tunneled in an IPv4 packet, the management ACLs are applied first on the external IPv4 header (rules with service field are ignored), and then again on the inner IPv6 header.

Example

The following example creates a management access list called 'mlist', configures management Ethernet interfaces e1 and e9 and makes the new access list the active list.

```
console# configure
console(config)# management access-list mlist
console(config-macl)# permit ip-source 192.168.200.1
console(config-macl)# exit
```

management access-class

The **management access-class** Global Configuration mode command restricts management connections by defining the active management access list. Use the **no** form of this command to delete an Access List.

Syntax

management access-class {**console-only** | *name*}

no management access-class

Parameters

- *name*— Specifies the Access List name. (Range: 1-32 characters)
- **console-only—**Indicates that the device can be managed only from the console.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures an access list called ‘mlist’ as the management access list.

```
Console(config)# management access-class mlist
```

permit (management)

The **permit** Management Access-List Configuration mode command defines a permit rule.

Syntax

permit ip-source *ip-address* [**mask** *mask* | *prefix-length*]

Parameters

- *ip-address* — A valid source IP address.
- *mask* — A valid network mask of the source IP address.
- *prefix-length* — Number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0-32)
- *vlan* — The VLAN number.
- *port-channel* — The port-channel number.
- *service* — The service type condition.

Default Configuration

If no permit rule is defined, the default is set to deny.

Command Mode

Management Access-list Configuration mode.

User Guidelines

The system supports up to 128 management access rules.

Example

The following example permits all ports in the access list called ‘mlist’.

```
Console(config)# management access-list mlist
Console(config-macl)# permit ip-source 172.16.15.3 ethernet e3
```

deny (management)

The **deny** Management Access-List Configuration mode command defines a deny rule.

Syntax

deny ip-source *ip-address* [**mask** *mask* | *prefix-length*]

Parameters

- *ip-address* — A valid source IP address.
- *mask* — A valid network mask of the source IP address.
- *prefix-length* — Specifies the number of bits that comprise the source IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0-32)
- *vlan* — The VLAN number.
- *port-channel* — The port-channel number.
- *service* — The service type condition.

Default Configuration

This command has no default configuration.

Command Mode

Management Access-list Configuration mode

User Guidelines

The system supports up to 128 management access rules.

Example

The following example denies all ports in the access list called ‘mlist’.

```
Console(config)# management access-list mlist
Console(config-macl)# deny ip-source 172.16.15.3
```

show management access-list

The **show management access-list** Privileged EXEC mode command displays management access lists.

Syntax

show management access-list

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the ‘mlist’ management access list.

```
Console# show management access-list mlist
        permit ethernet e1
        permit ethernet e9
! (Note: all other access implicitly denied)
```

show management access-class

The **show management access-class** Privileged EXEC mode command displays the active management access list.

Syntax

show management access-class

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about the active management access list.

```
Console# show management access-class
Management access-class is enabled, using access list mlist
```

20

PHY Diagnostics Commands

test copper-port tdr

The **test copper-port tdr** Privileged EXEC mode command uses Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port.

Syntax

test copper-port tdr *interface*

Parameters

- *interface* — A valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The port to be tested should be shut down during the test, unless it is a combination port with fiber port active.

The maximum length of cable for the TDR test is 120 meters.

Example

The following example results in a report on the cable attached to port e3.

```
Console# test copper-port tdr e3
Cable is open at 64 meters
Console# est copper-port tdr g4
Can’t perform this test on fiber ports
```

show copper-ports tdr

The **show copper-ports** tdr Privileged EXEC mode command displays information on the last Time Domain Reflectometry (TDR) test performed on copper ports.

Syntax

show copper-ports tdr [*interface*]

Parameters

- *interface* — A valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The maximum length of cable for the TDR test is 120 meters.

Example

The following example displays information on the last TDR test performed on all copper ports.

```
Console# show copper-ports tdr

Port    Result      Length (meters)    Date
----    ------      ---------------    ----
e1      OK
e2      Short       50                 13:32:00 23 July 2005
e3      Test has not been performed
e4      Open        64                 13:32:00 23 July 2005
e5      Fiber       -                  -
```

show copper-ports cable-length

The **show copper-ports cable-length** Privileged EXEC mode command displays the estimated copper cable length attached to a port.

Syntax

show copper-ports cable-length [*interface*]

Parameters

- *interface* — A valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The port must be active and working in 1000M mode.

Example

The following example displays the estimated copper cable length attached to all ports.

```
Console# show copper-ports cable-length

Port     Length (meters)
----     ------------------
e1       < 50
e2       Copper not active
e3       110-140
g4       Fiber
```

show fiber-ports optical-transceiver

The **show fiber-ports optical-transceiver** Privileged EXEC mode command displays the optical transceiver diagnostics.

Syntax

show fiber-ports optical-transceiver [*interface*] [**detailed**]

Parameters

- *interface* — A valid Ethernet port.
- **detailed** — Display detailed diagnostics.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

To test optical transceivers, ensure a fiber link is present.

Example

The following example displays the optical transceiver diagnostics results.

```
Console# show fiber-ports optical-transceiver 21

                       Power
Port   Temp   Voltage  Current    Output  Input   TX Fault LOS
----   ----   -------  -------    ------  -----   ----     ---
e1     W      OK       E          OK      OK      OK       OK
e2     OK     OK       OK         OK      OK      E        OK
e3     Copper

Temp – Internally measured transceiver temperature.
Voltage - Internally measured supply voltage.
Current – Measured TX bias current.
Output Power – Measured TX output power.
Input Power – Measured RX received power.
Tx Fault – Transmitter fault
LOS – Loss of signal

Console# show fiber-ports optical-transceiver detailed

                        Power
Port   Temp     Voltage Current   Output Input   TX       LOS
       [C]      [Volt]  [mA]      [mWatt] [mWatt]
----   ----     ------- -------   ------ -----   -------
e1     48       5.15    50        1.789   1.789   No       No
e2     43       5.15    10        1.789   1.789   No       No
e3     Copper

Temp – Internally measured transceiver temperature.
Voltage - Internally measured supply voltage.
Current – Measured TX bias current.
```

```
Output Power – Measured TX output power in milliWatts
Input Power – Measured RX received power milliWatts
Tx Fault – Transmitter fault
LOS – Loss of signal
```

21

Port Channel Commands

interface port-channel

The **interface port-channel** Global Configuration mode command enters the Global Configuration mode to configure a specific port-channel.

Syntax

interface port-channel *port-channel-number*

Parameters

- *port-channel-number* — A valid port-channel number. (Range: 1-64)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Eight aggregated links can be defined with up to eight member ports per port-channel. The aggregated links' valid IDs are 1-8.

Example

The following example enters the context of port-channel number 1.

```
Console(config)# interface port-channel 1
```

interface range port-channel

The **interface range port-channel** Global Configuration mode command enters the Global Configuration mode to configure multiple port-channels.

Syntax

interface range port-channel {*port-channel-range* | **all**}

Parameters

- *port-channel-range* — List of valid port-channels to add. Separate nonconsecutive port-channels with a comma and no spaces. A hyphen designates a range of port-channels. (Range: 1-64)
- **all** — All valid port-channels.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range.

Example

The following example groups port-channels 1, 2 and 6 to receive the same command.

```
Console(config)# interface range port-channel 1-2,6
```

channel-group

The **channel-group** Interface Configuration (Ethernet) mode command associates a port with a port-channel. Use the **no** form of this command to remove a port from a port-channel.

Syntax

channel-group *port-channel-number* **mode** {**n** | **auto**}

no channel-group

Parameters

- *port-channel-number* — Specifies the number of the valid port-channel for the current port to join. (Range: 1-64)
- **on** — Forces the port to join a channel without an LACP operation.
- **auto** — Allows the port to join a channel as a result of an LACP operation.

Default Configuration

The port is not assigned to a port-channel.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example forces port e1 to join port-channel 1 without an LACP operation.

```
Console(config)# interface ethernet e1
Console(config-if)# channel-group 1 mode on
```

show interfaces port-channel

The **show interfaces port-channel** Privileged EXEC mode command displays port-channel information.

Syntax

show interfaces port-channel [*port-channel-number*]

Parameters

- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on all port-channels.

```
Console# show interfaces port-channel

Channel      Ports
-------      ---------------------------------
1            Active: e1, e2
2            Active: e10, e15 Inactive: e17
3            Active: e19, e24
```

22

Port Monitor Commands

port monitor

The **port monitor** Interface Configuration mode command starts a port monitoring session. Use the **no** form of this command to stop a port monitoring session.

Syntax

port monitor *src-interface* [**rx** | **tx**]

no port monitor *src-interface*

Parameters

- *src-interface* — Valid Ethernet port.
- **rx** — Monitors received packets only.
- **tx** — Monitors transmitted packets only.

Default Configuration

Monitors both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command enables traffic on one port to be copied to another port, or between the source port (src-interface) and a destination port (port being configured).

The following restrictions apply to ports configured as destination ports:

The port cannot be already configured as a source port.

The port cannot be a member in a port-channel.

An IP interface is not configured on the port.

GVRP is not enabled on the port.

The port is not a member of a VLAN, except for the default VLAN (will automatically be removed from the default VLAN).

The following restrictions apply to ports configured to be source ports:

- The port cannot be already configured as a destination port.
- Maximum number of source ports can be up to eight.

Example

The following example copies traffic for both directions (Tx and Rx) on port e8 (source port) to port e1 (destination port).

```
Console(config)# interface ethernet e1
Console(config-if)# port monitor e8
```

show ports monitor

The **show ports monitor** Privileged EXEC mode command displays the port monitoring status.

Syntax

show ports monitor

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows how the port monitoring status is displayed.

```
Console# show ports monitor

Source Port  Destination Port  Type         Status
-----------  ----------------  -----        ------
e1           e8                RX,TX        Active
```

23

QoS Commands

qos

The **qos** Global Configuration mode command enables quality of service (QoS) on the device. Use the **no** form of this command to disable QoS on the device.

Syntax

qos [basic | advanced]

no qos

Parameters

- **basic** — QoS basic mode.
- **advanced** — QoS advanced mode, which enables the full range of QoS configuration.

Default Configuration

The QoS basic mode is enabled.

Command Mode

Global Configuration mode

User Guidelines

In advanced mode the VPT of the frame might be changed to egress_queue*2.

Example

The following example enables QoS on the device.

```
Console(config)# qos basic
```

show qos

The **show qos** Privileged EXEC mode command displays the quality of service (QoS) mode for the device.

Syntax

show qos

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Trust mode is displayed if QoS is enabled in basic mode.

Example

The following example displays QoS attributes when QoS is enabled in basic mode on the device.

```
Console# show qos
Qos: basic
Basic trust: vpt
```

class-map

The **class-map** Global Configuration mode command creates or modifies a class map and enters the Class-map Configuration mode. Use the **no** form of this command to delete a class map.

Syntax

class-map *class-map-name* [**match-all** | **match-any**]

no class-map *class-map-name*

Parameters

- *class-map-name* — Specifies the name of the class map (Range: 0-32 characters).
- **match-all** — Checks that the packet matches all classification criteria in the class map match statement.
- **match-any** — Checks that the packet matches one or more classification criteria in the class map match statement.

Default Configuration

By default, the **match-all** parameter is selected.

Command Mode

Global Configuration mode

User Guidelines

The **class-map** Global Configuration mode command is used to define packet classification, marking and aggregate policing as part of a globally named service policy applied on a per-interface basis.

The Class-Map Configuration mode enables entering up to two **match** Class-map Configuration mode commands to configure the classification criteria for the specified class. If two **match** Class-map Configuration mode commands are entered, each should point to a different type of ACL (e.g., one to an IP ACL and one to a MAC ACL). Since packet classification is based on the order of the classification criteria, the order in which the **match** Class-Map Configuration mode commands are entered is important.

If there is more than one match statement in a **match-all** class map and the same classification field appears in the participating ACLs, an error message is generated.

NOTE A class map in match-all mode cannot be configured if it contains both an IP ACL and a MAC ACL with an ether type that is not 0x0800.

Example

The following example creates a class map called class1 and configures it to check that packets match all classification criteria in the class map match statement.

```
Console(config)# class-map class1 match-all
Console(config-cmap)#
```

show class-map

The **show class-map** Privileged EXEC mode command displays all class maps.

Syntax

show class-map [*class-map-name*]

Parameters

- *class-map-name* — Specifies the name of the class map to be displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example shows the class map for class1.

```
Console# show class-map class1
Class Map match-any class1 (id4)
```

match

The **match** Class-map Configuration mode command defines the match criteria for classifying traffic. Use the **no** form of this command to delete the match criteria.

Syntax

match access-group *acl-name*

no match access-group *acl-name*

Parameters

- *acl-name* — Specifies the name of an IP or MAC ACL. (Range: 0-32 characters) Use “” for empty string

Default Configuration

No match criterion is supported.

Command Mode

Class-map Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the match criterion for classifying traffic as an access group called ‘enterprise’ in a class map called ‘class1’.

```
Console (config)# class-map class1
Console (config-cmap)# match access-group enterprise
```

policy-map

The **policy-map** Global Configuration mode command creates a policy map and enters the Policy-map Configuration mode. Use the **no** form of this command to delete a policy map.

Syntax

policy-map *policy-map-name*

no policy-map *policy-map-name*

Parameters

- *policy-map-name* — Specifies the name of the policy map (Range: 0-32 characters).

Command Mode

Global Configuration mode

User Guidelines

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** Global Configuration mode command to specify the name of the policy map to be created or modified.

Class policies in a policy map can only be defined if match criteria has already been defined for the classes. Use the **class-map** Global Configuration and **match** Class-map Configuration commands to define the match criteria of a class.

Only one policy map per interface per direction is supported. A policy map can be applied to multiple interfaces and directions.

Example

The following example creates a policy map called 'policy1' and enters the Policy-map Configuration mode.

```
Console (config)# policy-map policy1
Console (config-pmap)#
```

class

The **class** Policy-map Configuration mode command defines a traffic classification and enters the Policy-map Class Configuration mode. Use the **no** form of this command to remove a class map from the policy map.

Syntax

class *class-map-name* [**access-group** *acl-name*]

no class *class-map-name*

Parameters

- c*lass-map-name* — Specifies the name of an existing class map. If the class map does not exist, a new class map will be created under the specified name (Range: 0-32 characters).
- *acl-name* — Specifies the name of an IP or MAC ACL.

Default Configuration

No policy map is defined.

Command Mode

Policy-map Configuration mode

User Guidelines

Before modifying a policy for an existing class or creating a policy for a new class, use the **policy-map** Global Configuration mode command to specify the name of the policy map to which the policy belongs and to enter the Policy-map Configuration mode.

Use the **service-policy** (Ethernet, Port-channel) Interface Configuration mode command to attach a policy map to an interface. Use an existing class map to attach classification criteria to the specified policy map and use the **access-group** parameter to modify the classification criteria of the class map.

If this command is used to create a new class map, the name of an IP or MAC ACL must also be specified.

Example

The following example defines a traffic classification called ‘class1’ with an access-group called ‘enterprise’. The class is in a policy map called policy1.

```
Console(config)# policy-map policy1
Console (config-pmap)# class class1 access-group enterprise
```

show policy-map

The **show policy-map** Privileged EXEC mode command displays the policy maps.

Syntax

show policy-map [*policy-map-name* [*class-name*]]

Parameters

- *policy-map-name* — Specifies the name of the policy map to be displayed.
- *class-name* — Specifies the name of the class whose QoS policies are to be displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all policy maps.

```
Console# show policy-map

Policy Map policy1
  class class1
    set Ip dscp 7
```

```
Policy Map policy2
  class class 2
    police 96000 4800 exceed-action drop
  class class3
    police 124000 96000 exceed-action policed-dscp-transmit
```

trust

The **trust** Policy-Map Class Configuration mode command configures the trust state, which selects the value QoS uses as the source of internal DSCP value. Use **no trust** in order to return to the default trust state.

Syntax

trust [**cos** | **dscp** | **cos-dscp**]

no trust

Parameters

- **cos—**QoS set the queue according to CoS to Queue Map.
- **dscp—**QoS derives the internal DSCP value by using the DSCP value from the ingress packet. This is the default when no keyword is specified.
- **cos-dscp—**If the packet is IP then acts as dscp, otherwise acts as cos.

Default Configuration

Not trusted

Command Mode

Policy-map Class Configuration mode

User Guidelines

- Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from others. For example, incoming traffic with certain DSCP values can be trusted. Configure a class map to match and trust the DSCP values in the incoming traffic.
- Trust values set with this command supersede trust values set on specific interfaces with the **qos trust** interface configuration command.
- The **trust** command is mutually exclusive with set policy-map class configuration command within the same policy map.
- Policy maps that contain **set** or **trust** policy-map class configuration commands or with access control list (ACL) classification to an egress interface cannot be attached by using the **service-policy** interface configuration command.
- If **trust cos** is specified, QoS maps a packet to a queue to the received or default port CoS value and the CoS-to-queue map.
- If **trust dscp** is specified, QoS maps the packet by using the DSCP value from the ingress packet.
- If **tcp-udp-port** is specified, QoS maps the packet to queue by using the TCP\UDP port value from the ingress packet and the tcp-udp-port-to-queue map.

Example

The following example configures the trust state for a class called ‘class1’ in a policy map called ‘policy1’.

```
Console (config)# policy-map policy1
Console (config-pmap)# class class1
Console (config-pmap-c)# trust cos dscp
```

set

The **set** Policy-map Class Configuration mode command sets new values in the IP packet.

Syntax

set {**dscp** *new-dscp* | **queue** *queue-id* | **cos** *new-cos*}

no set

Parameters

- *new-dscp* — Specifies a new DSCP value for the classified traffic. (Range: 0-63)
- *queue-id* — Specifies an explicit queue ID for setting the egress queue.
- *new-cos* — Specifies a new user priority for marking the packet. (Range: 0-7)

NOTE NOTE: In SPS2xx 'set cos' command will not affect regular IP traffic, it will affect only non IP traffic, unless the outgoing port is Gigabit port

Default Configuration

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

User Guidelines

This command is mutually exclusive with the **trust** Policy-map Class Configuration command within the same policy map.

Policy maps that contain **set** or **trust** Policy-map Class Configuration commands or that have ACL classifications cannot be attached to an egress interface by using the **service-policy** (Ethernet, Port-channel) Interface Configuration mode command.

To return to the Policy-map Configuration mode, use the **exit** command. To return to the Privileged EXEC mode, use the **end** command.

Example

The following example sets the DSCP value in the packet to 56 for classes in policy map called ‘policy1’.

```
Console (config)# policy-map policy1
Console (config-pmap)# set dscp 56
```

police

The **police** Policy-map Class Configuration mode command defines the policer for classified traffic. Use the **no** form of this command to remove a policer.

Syntax

police *committed-rate-bps committed-burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]

no police

Parameters

- *committed-rate-bps* — Specifies the average traffic rate (CIR) in bits per second (bps).
- *committed-burst-byte* — Specifies normal burst size (CBS) in bytes.
- **drop** — Indicates that when the rate is exceeded, the packet is dropped.
- **policed-dscp-transmit** — Indicates that when the rate is exceeded, the DSCP of the packet is remarked according to the policed-DSCP map as configured by the **qos map policed-dscp** Global Configuration mode command.

Default Configuration

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

User Guidelines

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

Example

The following example defines a policer for classified traffic. When the traffic rate exceeds 124,000 bps or the normal burst size exceeds 96000 bps, the packet is dropped. The class is called 'class1' and is in a policy map called 'policy1'.

```
Console (config)# policy-map policy1
Console (config-pmap)# class class1
Console (config-pmap-c)# police 124000 9600 exceed-action drop
```

qos aggregate-policer

The **qos aggregate-policer** Global Configuration mode command defines the policer parameters that can be applied to multiple traffic classes within the same policy map. Use the **no** form of this command to remove an existing aggregate policer.

Syntax

qos aggregate-policer *aggregate-policer-name committed-rate-bps excess-burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**} [**dscp** *dscp*]

no qos aggregate-policer

Parameters

- *aggregate-policer-name* — Specifies the name of the aggregate policer.
- *committed-rate-bps* — Specifies the average traffic rate (CIR) in bits per second (bps).
- *excess-burst-byte* — Specifies the normal burst size (CBS) in bytes.
- **drop** — Indicates that when the rate is exceeded, the packet is dropped.
- **policed-dscp-transmit** — Indicates that when the rate is exceeded, the DSCP of the packet is remarked.
- *dscp* — Specifies the value that the DSCP is remarked. If unspecified, the DSCP is remarked according to the policed-DSCP map as configured by the **qos map policed-dscp** Global Configuration mode command.

Parameters Range

committed-rate-kbps — 3-57982058

committed -burst-byte — 3000-19173960

Default Configuration

No aggregate policer is defined.

Command Mode

Global Configuration mode

User Guidelines

Policers that contain **set** or **trust** Policy-map Class Configuration commands or that have ACL classifications cannot be attached to an output interface.

Define an aggregate policer if the policer is shared with multiple classes.

Policers in one port cannot be shared with other policers in another device; traffic from two different ports can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map; An aggregate policer cannot be applied across multiple policy maps.

This policer can also be used in Cascade police to make a cascade policer.

An aggregate policer cannot be deleted if it is being used in a policy map. The **no police aggregate** Policy-map Class Configuration command must first be used to delete the aggregate policer from all policy maps.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

show qos aggregate-policer

The **show qos aggregate-policer** Privileged EXEC mode command displays the aggregate policer parameter.

Syntax

show qos aggregate-policer [*aggregate-policer-name*]

Parameters

- *aggregate-policer-name* — Specifies the name of the aggregate policer to be displayed.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines.

Example

The following example displays the parameters of the aggregate policer called ‘policer1’.

```
Console# show qos aggregate-policer policer1
aggregate-policer policer1 96000 4800 exceed-action drop
not used by any policy map
```

police aggregate

The **police aggregate** Policy-map Class Configuration mode command applies an aggregate policer to multiple classes within the same policy map. Use the **no** form of this command to remove an existing aggregate policer from a policy map.

Syntax

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

Parameters

- *aggregate-policer-name* — Specifies the name of the aggregate policer.

Default Configuration

This command has no default configuration.

Command Mode

Policy-map Class Configuration mode

User Guidelines

An aggregate policer can be applied to multiple classes in the same policy map; An aggregate policer cannot be applied across multiple policy maps or interfaces.

To return to the Policy-map Configuration mode, use the **exit** command. To return to the Privileged EXEC mode, use the **end** command.

Example

The following example applies the aggregate policer called ‘policer’1 to a class called ‘class1’ in policy map called ‘policy1’.

```
Console(config)# policy-map policy1
Console(config-pmap)# class class1
Console(config-pmap-c)# police aggregate policer1
```

wrr-queue bandwidth

The **wrr-queue bandwidth** Global Configuration mode command assigns Weighted Round Robin (WRR) weights to egress queues. The weights ratio determines the frequency used by the packet scheduler to dequeue packets from each queue. Use the **no** form of this command to restore the default values.

Syntax

wrr-queue bandwidth *weight1 weight2 ... weight_n*

no wrr-queue bandwidth

Parameters

weight1 weight2 ... weight_n — Sets the ratio of the frequency in which the WRR packet scheduler de-queues packets. Separate each value by a space. The range is 0–65535.

Default Configuration

The default WRR weight is 1/4 the ratio for all queues (each weight set to 1).

Command Mode

Global Configuration mode

User Guidelines

The ratio for each queue is defined by the queue weight divided by the sum of all queue weights (also referred to as the normalized weight). This command sets the ratio of the frequency in which the WRR packet scheduler de-queues packets, and not the bandwidth. In other words, the ratio is of the number of packets and not the bytes sent from each queue.

A weight of 0 means no bandwidth is allocated for the same queue, and the share bandwidth is divided among the remaining queues.

All queues participate in the WRR queue scheme.

Example

The following example assigns a weight of 6 to each of the 8 WRR queues.

```
Console(config-if)# wrr-queue bandwidth 6 6 6 6
```

wrr-queue cos-map

The **wrr-queue cos-map** Global Configuration mode command maps Class of Service (CoS) values to a specific egress queue. Use the **no** form of this command to restore the default configuration.

Syntax

wrr-queue cos-map *queue-id cos1...cos8*

no wrr-queue cos-map [*queue-id*]

Parameters

- *queue-id* — Specifies the queue number to which the CoS values are mapped.
- *cos1...cos8* — Specifies CoS values to be mapped to a specific queue. (Range: 0-7)

Default Configuration

CoS values are mapped to 8 queues as follows:

Cos0 is mapped to queue 3.
Cos1 is mapped to queue 1.
Cos2 is mapped to queue 2.
Cos3 is mapped to queue 4.
Cos4 is mapped to queue 5.
Cos5 is mapped to queue 6.
Cos6 is mapped to queue 7.
Cos7 is mapped to queue 8.

Command Mode

Global Configuration mode

User Guidelines

This command can be used to distribute traffic into different queues, where each queue is configured with different Weighted Round Robin (WRR) and Weighted Random Early Detection (WRED) parameters.

It is recommended to specifically map a single VPT to a queue, rather than mapping multiple VPTs to a single queue. Use the **priority-queue out** Interface Configuration (Ethernet, Port-channel) mode command to enable expedite queues.

Example

The following example maps CoS 7 to queue 2.

```
Console(config)# wrr-queue cos-map 2 7
```

priority-queue out num-of-queues

The **priority-queue out num-of-queues** Global Configuration mode command configures the number of expedite queues. Use the **no** form of this command to restore the default configuration.

Syntax

priority-queue out num-of-queues *number-of-queues*

no priority-queue out num-of-queues

Parameters

- *number-of-queues* — Specifies the number of expedite queues. Expedite queues have higher indexes. (Range: 0-8)

Default Configuration

All queues are expedite queues.

Command Mode

Global Configuration mode

User Guidelines

Configuring the number of expedite queues affects the Weighted Round Robin (WRR) weight ratio because fewer queues participate in the WRR.

Example

The following example configures the number of expedite queues as 0.

```
Console(config)# priority-queue out num-of-queues 0
```

traffic-shape

The **traffic-shape** Interface Configuration (Ethernet, port-channel) mode command configures the shaper of the egress port/queue. Use the **no** form of this command to disable the shaper.

Syntax

traffic-shape {*committed-rate excess-burst*} [*queue-id*]

no traffic-shape [*queue-id*]

Parameters

- *committed-rate* — Specifies the average traffic rate (CIR) in bits per second (bps). (CIR range: 64–62500 Kbps,
  CBS: 8192-16769020 bytes)
- *excess-burst* — Specifies the excess burst size (CBS) in bytes.
- *queue-id* — Specifies the queue number to which the shaper is assigned.

Default Configuration

No shape is defined.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command activates the shaper on a specified egress port or egress queue.

To activate the shaper on an egress port, enter the Interface Configuration mode and specify the port number. Then run this command without the **queue-id** parameter. The CIR and the CBS will be applied to the specified port.

To activate the shaper for specific queue, run this command with the **queue-id** parameter.

Example

The following example sets a shaper on Ethernet port e5 when the average traffic rate exceeds 124000 bps or the normal burst size exceeds 96000 bps.

```
Console(config)# interface ethernet e5
Console(config-if) traffic-shape 124000 96000
```

rate-limit (Ethernet)

The **rate-limit** interface configuration command limits the rate of the incoming traffic. The **no** form of this command is used to disable the rate limit.

Syntax

rate-limit *kbps*

no rate-limit

Parameters

- *kbps* — Maximum of kilobits per second of ingress traffic on a port. (Range: 3.5M - 1G for SPS2024 and 62-100000 for SPS2xx)

Default Configuration

The default configuration is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The command can be enabled on a specific port only if the **port storm-control broadcast enable** interface configuration command is not enabled on that port.

Example

The following example limits the rate of the incoming traffic.

```
Console(config)# interface ethernet e5
Console(config-if) rate-limit
```

show qos interface

The **show qos interface** Privileged EXEC mode command displays Quality of Service (QoS) information on the interface.

Syntax

show qos interface [**buffers** | **queuing** | **policers** | **shapers** | **rate-limit**] [**Ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]

Parameters

- **ethernet** *interface-number* — Valid Ethernet port number.
- **lan** *vlan-id* — VLAN number.
- **port-channel** *number* — Valid port-channel number.
- **buffers** — Displays buffer setting for the interface's queues. For gigabit Ethernet displays, the queue depth for each of the 8 queues and the thresholds for the WRED/Tail Drop. For 10/100 displays the minimum reserved setting.
- **queuing** — Displays the queue's strategy (WRR or EF) and the weight for WRR queues and the CoS to queue map and the EF priority.
- **policers** — Displays all the policers configured for this interface, their setting, and the number of policers currently unused.
- **shapers** — Displays the shaper of the specified interface and the shaper for the queue on the specified interface.
- **rate-limit** — Displays the rate-limit configuration.

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

If no keyword is specified, port QoS mode (for example., DSCP trusted, CoS trusted, untrusted), default CoS value, DSCP-to-DSCP-mutation map attached to the port, and policy map attached to the interface are displayed.

If no interface is specified, QoS information about all interfaces is displayed.

Example

The following example displays the buffer settings for queues on Ethernet port e1.

```
Console# show qos interface ethernet e1 buffers

Ethernet e1
Notify Q Depth


qid      Size

1        125
2        125
3        125
4        125
5        125
6        125
7        125
8        125
```

```
qid                                     Threshold

1                                       100
2                                       100
3                                       100
4                                       100
5                                       N/A
6                                       N/A
7                                       N/A
8                                       N/A

qid   Min  Max  Prob  Min  Max  Prob  Min  Max  Prob   Weight
      DP0  DP0  DP0   DP1  DP1  DP1   DP2  DP2  DP2

1     N/A  N/A  N/A   N/A  N/A  N/A   N/A  N/A  N/A    N/A
2     N/A  N/A  N/A   N/A  N/A  N/A   N/A  N/A  N/A    N/A
3     N/A  N/A  N/A   N/A  N/A  N/A   N/A  N/A  N/A    N/A
4     N/A  N/A  N/A   N/A  N/A  N/A   N/A  N/A  N/A    N/A
5     50   60   13    65   80   6     85   95   4      2
6     50   60   13    65   80   6     85   95   4      2
7     50   60   13    65   80   6     85   95   4      2
8     50   60   13    65   80   6     85   95   4      2
```

qos wrr-queue threshold

The **wrr-queue threshold** Global Configuration mode command assigns queue thresholds globally. Use the **no** form of this command to restore the default configuration.

Syntax

qos wrr-queue threshold gigabitethernet *queue-id threshold-percentage0 threshold-percentage1 threshold-percentage2*

no qos wrr-queue threshold gigabitethernet *queue-id*

qos wrr-queue threshold tengigabitethernet *queue-id threshold-percentage0 threshold-percentage1 threshold-percentage2*

no qos wrr-queue threshold tengigabitethernet *queue-id*

Parameters

- **gigabitethernet** — Indicates that the thresholds are to be applied to Gigabit Ethernet ports.
- **tengigabitethernet** — Indicates that the thresholds are to be applied to 10 Gigabit Ethernet ports.
- *queue-id* — Specifies the queue number to which the threshold is assigned.
- *threshold-percentage0, 1,2* — Specifies the queue threshold percentage value. Each value is separated by a space. (Range: 0-100)

Default Configuration

80 percent for all thresholds.

Command Mode

Global Configuration mode.

User Guidelines

The packet refers to a certain threshold by the conformance level. If threshold 0 is exceeded, packets with the corresponding DP are dropped until the threshold is no longer exceeded. However, packets assigned to threshold 1 or 2 continue to be queued and sent as long as the second or third threshold is not exceeded.

Example

The following example assigns a threshold of 80 percent to WRR queue 1.

```
Console (config)# qos wrr-queue threshold gigabitethernet 1 80
```

qos map policed-dscp

The **qos map policed-dscp** Global Configuration mode command modifies the policed-DSCP map for remarking purposes. Use the **no** form of this command to restore the default map.

Syntax

qos map policed-dscp *dscp-list* **to** *dscp-mark-down*

no qos map policed-dscp

Parameters

- *dscp- list* — Specifies up to 8 DSCP values separated by a space. (Range: 0-63)
- *dscp-mark-down* — Specifies the DSCP value to mark down. (Range: 0-63)

Default Configuration

The default map is the **Null** map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode.

User Guidelines

DSCP values 3,11,19... cannot be remapped to other values.

Example

The following example marks down incoming DSCP value 3 as DSCP value 43 on the policed-DSCP map.

```
Console(config)# qos map policed-dscp 3 to 43
Reserved DSCP. DSCP 3 was not configured.
```

qos map dscp-queue

The **qos map dscp-queue** Global Configuration mode command modifies the DSCP to CoS map. Use the **no** form of this command to restore the default map.

Syntax

qos map dscp-queue *dscp-list* **to** *queue-id*

no qos map dscp-queue

Parameters

- *dscp-list* — Specifies up to 8 DSCP values separated by a space. (Range: 0 - 63)
- *queue-id* — Specifies the queue number to which the DSCP values are mapped.

Default Configuration

The following table describes the default map.

DSCP Value	0-7	8-15	16-23	24-31	32-39	40-47	48-56	57-63
Queue-ID	1	2	3	4	5	6	7	8

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
Console(config)# qos map dscp-queue 33 40 41 to 1
```

qos map dscp-dp

The **qos map dscp-dp** Global Configuration mode command maps the DSCP to Drop Precedence. Use the **no** form of this command to restore the default configuration.

Advanced mode only.

Syntax

qos map dscp-dp *dscp-list* **to** *dp*

no qos map dscp-dp [*dscp-list*]

Parameters

- *dscp-list* — Specifies up to 8 DSCP values, with each value separated by space. (Range: 0-63)
- *dp* — Enters the Drop Precedence value to which the DSCP values corresponds. (Range: 0-2, where 2 is the highest Drop Precedence)

In Cheetah based products

- *dp* — Enters the Drop Precedence value to which the DSCP values corresponds. Possible values are 0 - 1 (Where 1 is the highest Drop Precedence). (Range: 0-1)

Default Configuration

All the DSCPs are mapped to Drop Precedence 0.

Command Mode

Global Configuration mode.

User Guidelines

There are no user guidelines for this command.

Example

The following example displays how to priorities dscp values within the same queue.

```
Console(config)# qos map dscp-dp 30 to 0
```

qos trust (Global)

The **qos trust** Global Configuration mode command configures the system to the basic mode and trust state. Use the **no** form of this command to return to the untrusted state.

Syntax

qos trust {**cos** | **dscp**}

no qos trust

Parameters

- **cos** — Indicates that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- **dscp** — Indicates that ingress packets are classified with packet DSCP values.

Default Configuration

CoS is the default trust mode.

Command Mode

Global Configuration mode

User Guidelines

Packets entering a quality of service (QoS) domain are classified at the edge of the QoS domain. When packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every device in the domain.

A switch port on an inter-QoS domain boundary can be configured to the DSCP trust state, and, if the DSCP values are different between the QoS domains, the DSCP to DSCP mutation map can be applied.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When the system is configured as trust DSCP, traffic is mapped to a queue according to the DSCP-queue map.

Example

The following example configures the system to the DSCP trust state.

```
Console(config)# qos trust dscp
```

qos trust (Interface)

The **qos trust** Interface Configuration (Ethernet, port-channel) mode command enables each port trust state while the system is in the basic QoS mode. Use the **no** form of this command to disable the trust state on each port.

Syntax

qos trust

no qos trust

Default Configuration

qos trust is enabled on each port when the system is in basic mode.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures Ethernet port e15 to the default trust state.

```
Console(config)# interface ethernet e15
Console(config-if) qos trust
```

qos cos

The **qos cos** Interface Configuration (Ethernet, port-channel) mode command defines the default CoS value of a port. Use the **no** form of this command to restore the default configuration.

Syntax

qos cos *default-cos*

no qos cos

Parameters

- *default-cos* — Specifies the default CoS value of the port. (Range: 0-7)

Default Configuration

Default CoS value of a port is 0.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

If the port is trusted, the default CoS value of the port is used to assign a CoS value to all untagged packets entering the port.

Example

The following example configures port e15 default CoS value to **3**.

```
Console(config)# interface ethernet e15
Console(config-if) qos cos 3
```

qos dscp-mutation

The **qos dscp-mutation** Global Configuration mode command applies the DSCP Mutation map to a system DSCP trusted port. Use the **no** form of this command to restore the trust state with no DSCP mutation.

Syntax

qos dscp-mutation

no qos dscp-mutation

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode.

User Guidelines

The DSCP to DSCP mutation map is applied to a port at the boundary of a Quality of Service (QoS) administrative domain.

If two QoS domains have different DSCP definitions, use the DSCP to DSCP mutation map to match one set of DSCP values with the DSCP values of another domain.

Apply the DSCP to DSCP mutation map only to ingress and to DSCP-trusted ports. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports.

If the DSCP to DSCP mutation map is applied to an untrusted port, class of service (CoS) or IP-precedence trusted port, this command has no immediate effect until the port becomes DSCP-trusted.

Example

The following example applies the DSCP Mutation Map to system DSCP trusted ports.

```
Console(config)# qos dscp-mutation
```

qos map dscp-mutation

The **qos map dscp-mutation** Global Configuration mode command modifies the DSCP to DSCP mutation map. Use the **no** form of this command to restore the default DSCP to DSCP mutation map.

Syntax

qos map dscp-mutation *in-dscp* **to** *out-dscp*

no qos map dscp-mutation

Parameters

- *in-dscp* — Specifies up to 8 DSCP values separated by spaces. (Range: 0-63)
- *out-dscp* — Specifies up to 8 DSCP values separated by spaces. (Range: 0-63)

Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode.

User Guidelines

This is the only map that is not globally configured. it is possible to have several maps and assign each one to different ports.

Example

The following example changes DSCP values 1, 2, 4, 5 and 6 to DSCP Mutation Map value 63.

```
Console(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

show qos map

The **show qos map** Global Configuration mode command displays the QoS mapping information.

Syntax

show qos map [dscp-queue | dscp-dp | policed-dscp | dscp-mutation

Parameters

- **dscp-queue** — Displays the DSCP to queue map.
- **dscp-dp** — Displays the DSCP to Drop Precedence map.
- **policed-dscp** — Displays the DSCP to DSCP remark table.
- **dscp-mutation** — Displays the DSCP-DSCP mutation table.

Default Configuration

The default configuration is set to disabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the QoS mapping information.

```
Console> show qos map

Dscp-queue map:

dl    :   d2   0    1   2    3    4   5    6    7   8    9
--    --  --   --   --  --   --   --  --   --   --  --   --
0              01   01  01   01   01  01   01   01  01   01
1              01   01  01   01   01  01   02   02  02   02
2              02   02  02   02   02  02   02   02  02   02
3              02   02  03   03   03  03   03   03  03   03
4              03   03  03   03   03  03   03   03  04   04
5              04   04  04   04   04  04   04   04  04   04
6              04   04  04   04
```

```
Dscp-DP map:

dl        :    d2  0   1    2    3   4    5     6   7   8   9
--        --   --  --  --   --   --  --   --    --  --  --  --
0                  00  00   00   00  00   00    00  00  00  00
1                  00  00   00   00  00   00    00  00  00  00
2                  00  00   00   00  00   00    00  00  00  00
3                  00  00   00   00  00   00    00  00  00  00
4                  00  00   00   00  00   00    00  00  00  00
5                  00  00   00   00  00   00    00  00  00  00
6                  00  00   00   00


Dscp-dscp mutation map:

dl        :    d2  0   1    2    3   4    5     6   7   8   9
--        --   --  --  --   --   --  --   --    --  --  --  --
0                  00  01   02   03  04   05    06  07  08  09
1                  10  11   12   13  14   15    16  17  18  19
2                  20  21   22   23  24   25    26  27  28  29
3                  30  31   32   33  34   35    36  37  38  39
4                  40  41   42   43  44   45    46  47  48  49
5                  50  51   52   53  54   55    56  57  58  59
6                  60  61   62   63  64   65    66  67  68  69
```

24

RADIUS Commands

radius-server host

The **radius-server host** Global Configuration mode command specifies a RADIUS server host. Use the **no** form of this command to delete the specified RADIUS host.

Syntax

radius-server host {*ip-address* | *hostname*} [**auth-port** *auth-port-number*] [**acct-port** *acct-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**source** *source*] [**priority** *priority*] [**usage** *type*]

no radius-server host {*ip-address* | *hostname*}

Parameters

- *ip-address* — IP address of the RADIUS server host.
- *hostname* — Hostname of the RADIUS server host. (Range: 1-158 characters)
- *auth-port-number* — Port number for authentication requests. The host is not used for authentication if the port number is set to 0. (Range: 0-65535)
- *acct-port-number* — Port number for accounting requests. The host is not used for accountings if set to 0.
- *timeout* — Specifies the timeout value in seconds. (Range: 1-30)
- *retries* — Specifies the retransmit value. (Range: 1-10)
- *deadtime* — Length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0-2000)
- *key-string* — Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This

key must match the encryption used on the RADIUS daemon. To specify an empty string, enter “”. (Range: 0-128 characters)

- *source* — Specifies the source IP address to use for communication. 0.0.0.0 is interpreted as request to use the IP address of the outgoing IP interface.
- *priority* — Determines the order in which servers are used, where 0 has the highest priority. (Range: 0-65535)
- *type* — Specifies the usage type of the server. Possible values: **login**, **dot.1x**, **wireless** or **all**.

Default Configuration

No RADIUS server host is specified.

The port number for authentication requests is 1812.

The port number for accounting requests if not specified is 1813

The usage type is **all**.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, multiple **radius-server host** commands can be used.

If no host-specific timeout, retries, deadtime or key-string values are specified, global values apply to each RADIUS server host.

The address type of the source parameter must be the same as the *ip-address* parameter.

Example

The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20 and a 20-second timeout period.

```
Console(config)# radius-server host 192.168.10.1 auth-port 20
timeout 20
```

radius-server key

The **radius-server key** Global Configuration mode command sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server key [*key-string*]

no radius-server key

Parameters

- *key-string* — Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon.

(Range: 0-128 characters)

Default Configuration

The key-string is an empty string.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.

```
Console(config)# radius-server key enterprise-server
```

radius-server retransmit

The **radius-server retransmit** Global Configuration mode command specifies the number of times the software searches the list of RADIUS server hosts. Use the **no** form of this command to reset the default configuration.

Syntax

radius-server retransmit *retries*

no radius-server retransmit

Parameters

- *retries* — Specifies the retransmit value. (Range: 1-10)

Default Configuration

The software searches the list of RADIUS server hosts 3 times.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the number of times the software searches all RADIUS server hosts to 5 times.

```
console(config)# radius-server retransmit 5
```

radius-server source-ip

The **radius-server source-ip** Global Configuration mode command specifies the source IP address used for communication with RADIUS servers. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server source-ip *source*

no radius-source-ip *source*

Parameters

- *source* — Specifies a valid source IP address.

Default Configuration

The source IP address is the IP address of the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the source IP address used for communication with all RADIUS servers to 10.1.1.1.

```
console(config)# radius-server source-ip 10.1.1.1
```

radius-server timeout

The **radius-server timeout** Global Configuration mode command sets the interval during which the device waits for a server host to reply. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server timeout *timeout*

no radius-server timeout

Parameters

- *timeout* — Specifies the timeout value in seconds. (Range: 1-30)

Default Configuration

The timeout value is **3** seconds.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the timeout interval on all RADIUS servers to 5 seconds.

```
Console(config)# radius-server timeout 5
```

radius-server deadtime

The **radius-server deadtime** Global Configuration mode command improves RADIUS response time when servers are unavailable. The command is used to cause the unavailable servers to be skipped. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

Parameters

- *deadtime* — Length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0-2000)

Default Configuration

The deadtime setting is **0**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets all RADIUS server deadtimes to 10 minutes.

```
Console(config)# radius-server deadtime 10
```

show radius-servers

The **show radius-servers** Privileged EXEC mode command displays the RADIUS server settings.

Syntax

show radius-servers

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays RADIUS server settings.

```
Console# show radius-servers

IP address Port TimeOut RetransmitDeadTimeSource IPPriorityUsage
           Auth
---------- ---- ------- ----------------- -------- -------------
172.16.1.1 1645 Global  Global    Global  -        1          All
172.16.1.2 1645 11      8         Global  Global   2          All

Global values
-------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IP: 172.16.8.1
```

25

RMON Commands

show rmon statistics

The **show rmon statistics** Privileged EXEC mode command displays RMON Ethernet statistics.

Syntax

show rmon statistics {**ethernet** *interface number* | **port-channel** *port-channel-number*}

Parameters

- *interface number* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays RMON Ethernet statistics for Ethernet port e1.

```
Console# show rmon statistics ethernet e1
RMPort: e1
Dropped: 8
Octets: 878128                Packets: 978
Broadcast: 7                  Multicast: 1
CRC Align Errors: 0           Collisions: 0
Undersize Pkts: 0             Oversize Pkts: 0
Fragments: 0                  Jabbers: 0
64 Octets: 98                 65 to 127 Octets: 0
128 to 255 Octets: 0          256 to 511 Octets: 0
512 to 1023 Octets: 491       1024 to 1518 Octets: 389
```

The following table describes the significant fields shown in the display.

Field	Description
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, Broadcast packets, and Multicast packets) received.
Broadcast	The total number of good packets received and directed to the Broadcast address. Does not include Multicast packets.
Multicast	The total number of good packets received and directed to a Multicast address. This number does not include packets directed to the Broadcast address.
CRC Align Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Field	Description
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Undersize Pkts	The total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	The total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	The total number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	The total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
64 Octets	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	The total number of packets (including bad packets) received that are between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 Octets to max	The total number of packets (including bad packets) received that were between 1024 and maximum frame size in length inclusive (excluding framing bits but including FCS octets).

rmon collection history

The **rmon collection history** Interface Configuration (Ethernet, port-channel) mode command enables a Remote Monitoring (RMON) MIB history statistics group on an interface. Use the **no** form of this command to remove a specified RMON history statistics group.

Syntax

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

Parameters

- *index* — Specifies the statistics group index. (Range: 1-65535)
- *ownername* — Specifies the RMON statistics group owner name. (Range: 0-160 characters)
- *bucket-number* — Number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50. (Range:1-65535)
- *seconds* — Number of seconds in each polling cycle. (Range: 1-3600)

Default Configuration

RMON statistics group owner name is an empty string.

Number of buckets specified for the RMON collection history statistics group is 50.

Number of seconds in each polling cycle is 1800.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

Cannot be configured for a range of interfaces (Range context).

Example

The following example enables a Remote Monitoring (RMON) MIB history statistics group on Ethernet port e1 with index number 1 and a polling interval period of 2400 seconds.

```
Console(config)# interface ethernet e1
Console(config-if)# rmon collection history 1 interval 2400
```

show rmon collection history

The **show rmon collection history** Privileged EXEC mode command displays the requested RMON history group statistics.

Syntax

show rmon collection history [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — Valid Ethernet port.
- *port-channel-number* — Valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all RMON history group statistics.

```
Console# show rmon collection history

Index Interface Interval Requested Granted Owner
                         Samples   Samples
----- --------- -------- --------- ------- -------
1     e1        30       50        50      CLI
2     e1        1800     50        50      Manager
```

The following table describes the significant fields shown in the display.

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry

show rmon history

The **show rmon history** Privileged EXEC mode command displays RMON Ethernet history statistics.

Syntax

show rmon history *index* {**throughput** | **errors** | **other**} [**period** seconds]

Parameters

- *index* — Specifies the requested set of samples. (Range: 1-65535)

- **throughput** — Indicates throughput counters.
- **errors** — Indicates error counters.
- **other** — Indicates drop and collision counters.
- *seconds* — Specifies the period of time in seconds. (Range: 1-4294967295)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays RMON Ethernet history statistics for index 1.

```
Console# show rmon history 1 throughput

Sample Set: 1            Owner: CLI
Interface: e1            Interval: 1800
Requested Samples: 50Granted Samples: 50

Maximum Table Size: 500

Time                 Octets    Packets  Broadcast Multicast Util
-------------------- --------- -------  --------- --------- ----
Jan 18 2005 21:57:00 303595962 357568   3289      7287      19%
Jan 18 2005 21:57:30 287696304 275686   2789      5878      20%


Console# show rmon history 1 errors
```

```
Sample Set: 1                 Owner: Me
Interface: e1                 Interval: 1800
Requested Samples: 50Granted Samples: 50

Maximum Table Size: 500 (800 after reset)

Time                CRC Align Undersize Oversize Fragments Jabbers

---------------------------- --------- ------- -------- -------
---

Jan 18 2005 21:57:00 1                  1                 0490
Jan 18 2005 21:57:30 1                  1                 0270
```

```
Console# show rmon history 1 other

Sample Set: 1                         Owner: Me
Interface: e1                         Interval: 1800
Requested Samples: 50Granted Samples: 50

Maximum Table Size: 500

Time                     Dropped  Collisions
-------------------      -------  ----------
Jan 18 2005 21:57:00     3        0
Jan 18 2005 21:57:30     3        0
```

Field	Description
Time	Date and Time the entry is recorded.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The number of packets (including bad packets) received during this sampling interval.
Broadcast	The number of good packets received during this sampling interval that were directed to the Broadcast address.
Multicast	The number of good packets received during this sampling interval that were directed to a Multicast address. This number does not include packets addressed to the Broadcast address.

Field	Description
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Oversize	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (AlignmentError). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.

Field	Description
Collisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

rmon alarm

The **rmon alarm** Global Configuration mode command configures alarm conditions. Use the **no** form of this command to remove an alarm.

Syntax

rmon alarm *index variable interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]

no rmon alarm *index*

Parameters

- *index* — Specifies the alarm index. (Range: 1-65535)
- *variable* — Specifies the object identifier of the variable to be sampled.
- *interval* — Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 0-2147483647)
- *rthreshold* — Specifies the rising threshold. (Range: 0-2147483647)
- *fthreshold* — Specifies the falling threshold. (Range: 0-2147483647)
- *revent* — Specifies the event index used when a rising threshold is crossed. (Range: 1-65535)
- *fevent* — Specifies the event index used when a falling threshold is crossed. (Range: 1-65535)

- *type* — Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. Possible values are **absolute** and **delta**.

  If the method is **absolute**, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the method is **delta**, the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.

- direction — Specifies the alarm that may be sent when this entry is first set to valid. Possible values are **rising**, **rising-falling** and **falling**.

If the first sample (after this entry becomes valid) is greater than or equal to *rthreshold* and *direction* is equal to **rising** or **rising-falling**, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to *fthreshold* and *direction* is equal to falling or rising-falling, a single falling alarm is generated.

- *name* — Specifies the name of the person who configured this alarm. If unspecified, the name is an empty string.

Default Configuration

The type is **absolute**.

The startup direction is **rising-falling**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the following alarm conditions:

- Alarm index — 1000
- Variable identifier — LinkSys

- Sample interval — 360000 seconds
- Rising threshold — 1000000
- Falling threshold — 1000000
- Rising threshold event index — 10
- Falling threshold event index — 20

```
Console(config)# rmon alarm 1000 LinkSys 360000 1000000 1000000
10 20
```

show rmon alarm-table

The show **rmon alarm-table** Privileged EXEC mode command displays the alarms table.

Syntax

show rmon alarm-table

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the alarms table.

```
Console# show rmon alarm-table
```

```
Index   OID                     Owner
-----   ----------------        ------
1       1.3.6.1.2.1.2.2.1.10.1  CLI
2       1.3.6.1.2.1.2.2.1.10.1  Manager
3       1.3.6.1.2.1.2.2.1.10.9  CLI
```

The following table describes significant fields shown in the example:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

show rmon alarm

The **show rmon alarm** Privileged EXEC mode command displays alarm configuration.

Syntax

show rmon alarm *number*

Parameters

- *number* — Specifies the alarm index. (Range: 1-65535)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays RMON 1 alarms.

```
Console# show rmon alarm 1

Alarm 1
-------
Field   Value
OID     1.3.6.1.2.1.2.2.1.10.1
Last Sample Value878128
Interval30
Sample Typedelta
Startup Alarmrising
Rising Threshold8700000
Falling Threshold78
Rising Event1
Falling Event1
Owner   CLI
```

Field	Description
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	The statistic value during the last sampling period. For example, if the sample type is **delta**, this value is the difference between the samples at the beginning and end of the period. If the sample type is **absolute**, this value is the sampled value at the end of the period.
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.

Field	Description
Sample Type	The method of sampling the variable and calculating the value compared against the thresholds. If the value is **absolute**, the value of the variable is compared directly with the thresholds at the end of the sampling interval. If the value is **delta**, the value of the variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Startup Alarm	The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising and falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising and falling, then a single falling alarm is generated.
Rising Threshold	A sampled statistic threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	A sampled statistic threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	The event index used when a rising threshold is crossed.
Falling Event	The event index used when a falling threshold is crossed.
Owner	The entity that configured this entry.

rmon event

The **rmon event** Global Configuration mode command configures an event. Use the **no** form of this command to remove an event.

Syntax

rmon event *index type* [**community** *text*] [**description** *text*] [**owner** *name*]

no rmon event *index*

Parameters

- *index* — Specifies the event index. (Range: 1-65535)
- *type* — Specifies the type of notification generated by the device about this event. Possible values: **none**, **log**, **trap**, **log-trap**.
- **community** *text* — If the specified notification type is trap, an SNMP trap is sent to the SNMP community specified by this octet string. (Range: 0-127 characters)
- **description** *text* — Specifies a comment describing this event. (Range: 0-127 characters)
- *name* — Specifies the name of the person who configured this event. If unspecified, the name is an empty string.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

If log is specified as the notification type, an entry is made in the log table for each event. If **trap** is specified, an SNMP trap is sent to one or more management stations.

Example

The following example configures an event identified as index 10 and for which the device generates a notification in the log table.

```
Console(config)# rmon event 10 log
```

show rmon events

The **show rmon events** Privileged EXEC mode command displays the RMON event table.

Syntax

show rmon events

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the RMON event table.

```
Console# show rmon events

Index Description   Type Community Owner   Last time sent
----- ------------------ --------- ------- --------------
1     Errors        Log            CLI     Jan 18 2006 23:58:17
2     High BroadcastLog-Trapdevice Manager Jan 18 2006 23:59:48
```

The following table describes significant fields shown in the example:

Field	Description
Index	An index that uniquely identifies the event.
Description	A comment describing this event.
Type	The type of notification that the device generates about this event. Can have the following values: none, log, trap, log-trap. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last Time Sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

show rmon log

The **show rmon log** Privileged EXEC mode command displays the RMON log table.

Syntax

show rmon log [*event*]

Parameters

- *event* — Specifies the event index. (Range: 0-65535)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the RMON log table.

```
Console# show rmon log

Maximum table size: 500

Event      Description        Time
--------   --------------     ----------
1          Errors             Jan 18 2006 23:48:19
1          Errors             Jan 18 2006 23:48:19
2          High Broadcast     Jan 18 2006 23:48:19

Console# show rmon log

Maximum table size: 500 (800 after reset)

Event    Description          Time
-------- --------------       ----------
1       Errors                Jan 18 2006 23:48:19
1       Errors                Jan 18 2006 23:48:19
2       High Broadcast        Jan 18 2006 23:48:19
```

The following table describes the significant fields shown in the display:

Field	Description
Event	An index that uniquely identifies the event.
Description	A comment describing this event.
Type	The time this entry was created.

rmon table-size

The **rmon table-size** Global Configuration mode command configures the maximum size of RMON tables. Use the **no** form of this command to return to the default configuration.

Syntax

rmon table-size {**history** *entries* | **log** *entries*}

no rmon table-size {**history** | **log**}

Parameters

- **history** *entries* — Maximum number of history table entries. (Range: 20 - 32767)
- **log** *entries* — Maximum number of log table entries. (Range: 20-32767)

Default Configuration

History table size is **270**.

Log table size is **200**.

Command Mode

Global Configuration mode

User Guidelines

The configured table size takes effect after the device is rebooted.

Example

The following example configures the maximum RMON history table sizes to 100 entries.

```
Console(config)# rmon table-size history 100
```

SNMP Commands

snmp-server community

The **snmp-server community** Global Configuration mode command configures the community access string to permit access to the SNMP protocol. Use the **no** form of this command to remove the specified community string.

Syntax

snmp-server community *community* [**ro** | **rw** | **su**] [*ip-address*] [**view** *view-name*][**type router** | **oob**]

snmp-server community-group *community group-name* [*ip-address*] [**type router** | **oob**]

no snmp-server community *community* [*ip-address*]

Parameters

- *community* — Community string that acts like a password and permits access to the SNMP protocol. (Range: 1-20 characters)
- **ro** — Indicates read-only access (default).
- **rw** — Indicates read-write access.
- **su** — Indicates SNMP administrator access.
- *ip-address* — Specifies the IP address of the management station. (Range: Valid ip address)
- *group-name* — Specifies the name of a previously defined group. A group defines the objects available to the community. (Range: 1-30 characters)
- *view-name* — Specifies the name of a previously defined view. The view defines the objects available to the community. (Range: 1-30 characters).

- **type router** — Specifies that SNMP requests for duplicate tables configure the router tables. This is the default.
- **type oob** — Specifies that SNMP requests for duplicate tables configure the oob tables.

Default Configuration

No communities are defined.

Command Mode

Global Configuration mode

User Guidelines

The **view-name** parameter cannot be specified for **su**, which has access to the whole MIB.

The **view-name** parameter can be used to restrict the access rights of a community string. When it is specified:

An internal security name is generated.

The internal security name for SNMP**v1** and SNMP**v2** security models is mapped to an internal group name.

The internal group name for SNMP**v1** and SNMP**v2** security models is mapped to a view-name (read-view and notify-view always, and for **rw** for write-view also)

The **group-name** parameter can also be used to restrict the access rights of a community string. When it is specified:

An internal security name is generated.

The internal security name for SNMP**v1** and SNMP**v2** security models is mapped to the group name.

Example

The following example defines community access string **public** to permit administrative access to SNMP protocol at an administrative station with IP address 192.168.1.20.

```
Console(config)# snmp-server community public su 192.168.1.20
```

snmp-server view

The **snmp-server view** Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server view entry. Use the **no** form of this command to remove a specified SNMP server view entry.

Syntax

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name* [*oid-tree*]

Parameters

- *view-name* — Specifies the label for the view record that is being created or updated. The name is used to reference the record. (Range: 1-30 characters)
- *oid-tree* — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
- **included** — Indicates that the view type is included.
- **excluded** — Indicates that the view type is excluded.

Default Configuration

'Default' and 'DefaultSuper' views exists.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same view record.

The number of views is limited to 64.

No check is made to determine that a MIB node corresponds to the “starting portion” of the OID until the first wildcard.

Example

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group.

```
Console(config)# snmp-server view user-view system included
Console(config)# snmp-server view user-view system.7 excluded
Console(config)# snmp-server view user-view ifEntry.*.1 included
```

snmp-server group

The **snmp-server group** Global Configuration mode command configures a new Simple Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. Use the **no** form of this command to remove a specified SNMP group.

Syntax

snmp-server group *groupname* {**v1** | **2** | **v3** {**noauth** | **auth** | **priv**} [**notify** *notifyview*]} [**read** *readview*] [**write** *writeview*]

no snmp-server group *groupname* {**v1** | **v2** | **v3** [**noauth** | **auth** | **priv**]}

Parameters

- *groupname*—Specifies the name of the group (Range: 1-30 characters).
- **v1** — Indicates the SNMP Version 1 security model.
- **v2** — Indicates the SNMP Version 2 security model.
- **v3** — Indicates the SNMP Version 3 security model.
- **noauth** — Indicates no authentication of a packet. Applicable only to the SNMP Version 3 security model.
- **auth** — Indicates authentication of a packet without encrypting it. Applicable only to the SNMP Version 3 security model.
- **priv** — Indicates authentication of a packet with encryption. Applicable only to the SNMP Version 3 security model.
- *name* — Specifies the context of a packet. The following context is supported: Router. If the context name is unspecified, all contexts are defined.
- *notifyview* — Specifies a string that is the name of the view that enables specifying an inform or a trap. If unspecified, nothing is defined for the notify view. Applicable only to the SNMP Version 3 security model.
- *readview* — Specifies a string that is the name of the view that enables only viewing the contents of the agent. If unspecified, all objects except for the community-table and SNMPv3 user and access tables are available.
- *writeview* — Specifies a string that is the name of the view that enables entering data and configuring the contents of the agent. If unspecified, nothing is defined for the write view.

Default Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

The Router context is translated to “” context in the MIB.

Example

The following example attaches a group called user-group to SNMPv3 and assigns to the group the privacy security level and read access rights to a view called user-view.

```
Console(config)# snmp-server group user-group v3 riv read user-view
```

snmp-server user

The **snmp-server user** Global Configuration mode command configures a new SNMP Version 3 user. Use the **no** form of this command to remove a user.

Syntax

snmp-server user *username groupname* [**remote** *engineid-string*] [**auth-md5** *password* | **auth-sha** *password* | **auth-md5-key** *md5-des-keys* | **auth-sha-key** *sha-des-keys*]

no snmp-server user *username* [**remote** *engineid-string*]

Parameters

- *username* — Specifies the name of the user on the host that connects to the agent. (Range: 1-30 characters)
- *groupname* — Specifies the name of the group to which the user belongs. (Range: 1-30 characters)
- *engineid-string* — Specifies the engine ID of the remote SNMP entity to which the user belongs. The engine ID is a concatenated hexadecimal string. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (Range: 5-32 characters)

- **auth-md5** *password* — Indicates the HMAC-MD5-96 authentication level. The user should enter a password for authentication and generation of a DES key for privacy. (Range: 1-32 characters)
- **auth-sha** *password* — Indicates the HMAC-SHA-96 authentication level. The user should enter a password for authentication and generation of a DES key for privacy. (Range: 1-32 characters)
- **auth-md5-key** *md5-des-keys* — Indicates the HMAC-MD5-96 authentication level. The user should enter a concatenated hexadecimal string of the MD5 key (MSB) and the privacy key (LSB). If authentication is only required, 16 bytes should be entered; if authentication and privacy are required, 32 bytes should be entered. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (16 or 32 bytes)
- **auth-sha-key** *sha-des-keys* — Indicates the HMAC-SHA-96 authentication level. The user should enter a concatenated hexadecimal string of the SHA key (MSB) and the privacy key (LSB). If authentication is only required, 20 bytes should be entered; if authentication and privacy are required, 36 bytes should be entered. Each byte in the hexadecimal character string is two hexadecimal digits. Each byte can be separated by a period or colon. (20 or 36 bytes)

Default Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

If **auth-md5** or **auth-sha** is specified, both authentication and privacy are enabled for the user.

When a **show running-config** Privileged EXEC mode command is entered, a line for this user will not be displayed. To see if this user has been added to the configuration, type the **show snmp users** Privileged EXEC mode command.

An SNMP EngineID has to be defined to add SNMP users to the device. Changing or removing the SNMP EngineID value deletes SNMPv3 users from the device's database.

The remote engineid designates the remote management station and should be defined to enable the device to receive informs.

Example

The following example configures an SNMPv3 user named 'John' in a group called 'user-group'.

```
Console(config)# snmp-server user John user-group
```

snmp-server filter

The **snmp-server filter** Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server filter entry. Use the **no** form of this command to remove the specified SNMP server filter entry.

Syntax

snmp-server filter *filter-name oid-tree* {**included** | **excluded**}

no snmp-server filter *filter-name* [*oid-tree*]

Parameters

- *filter-name* — Specifies the label for the filter record that is being updated or created. The name is used to reference the record. (Range: 1-30 characters)
- *oid-tree* — Specifies the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included** — Indicates that the filter type is included.
- **excluded** — Indicates that the filter type is excluded.

Default Configuration

No filter entry exists.

Command Mode

Global Configuration mode

User Guidelines

This command can be entered multiple times for the same filter record. Later lines take precedence when an object identifier is included in two or more lines.

Example

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group.

```
Console(config)# snmp-server filter filter-name system included
Console(config)# snmp-server filter filter-name system.7
excluded
Console(config)# nmp-server filter filter-name ifEntry.*.1
included
```

snmp-server host

The **snmp-server host** Global Configuration mode command specifies the recipient of Simple Network Management Protocol Version 1 or Version 2 notifications. Use the **no** form of this command to remove the specified host.

Syntax

snmp-server host {*ip-address* | *hostname*} *community-string* [**traps** | **informs**] [**1** | **2**] [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]

no snmp-server host {*ip-address* | *hostname*} [**traps** | **informs**]

Parameters

- *ip-address* — Specifies the IP address of the host (targeted recipient).
- *hostname* — Specifies the name of the host. (Range:1-158 characters)
- *community-string* — Specifies a password-like community string sent with the notification operation. (Range: 1-20)
- **traps** — Indicates that SNMP traps are sent to this host. If unspecified, SNMP**v2** traps are sent to the host.
- **informs** — Indicates that SNMP informs are sent to this host. Not applicable to SNMP**v1**.
- **1** — Indicates that SNMP**v1** traps will be used.
- **2** — Indicates that SNMP**v2** traps will be used. If
- *port*—Specifies the UDP port of the host to use. If unspecified, the default UDP port number is 162. (Range:1-65535)
- *filtername* — Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
- *seconds* — Specifies the number of seconds to wait for an acknowledgment before resending informs. If unspecified, the default timeout period is **15** seconds. (Range: 1-300)
- *retries* — Specifies the maximum number of times to resend an inform request. If unspecified, the default maximum number of retries is **3**. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

When configuring an SNMP**v1** or SNMP**v2** notification recipient, a notification view for that recipient is automatically generated for all the MIB.

When configuring an SNMP**v1** notification recipient, the **Inform** option cannot be selected.

If a trap and inform are defined on the same target, and an inform was sent, the trap is not sent.

Example

The following example enables SNMP traps for host 10.1.1.1 with community string “management” using SNMPv2.

```
Console(config)# snmp-server host 10.1.1.1 management 2
```

snmp-server v3-host

The **snmp-server v3-host** Global Configuration mode command specifies the recipient of Simple Network Management Protocol Version 3 notifications. Use the **no** form of this command to remove the specified host.

Syntax

snmp-server v3-host {*ip-address* | *hostname*} *username* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]

no snmp-server v3-host {*ip-address* | *hostname*} *username* [**traps** | **informs**]

Parameters

- *ip-address* — Specifies the IP address of the host (targeted recipient).
- *hostname* — Specifies the name of the host. (Range:1-158 characters)
- *username* — Specifies the name of the user to use to generate the notification. (Range: 1-24)
- **traps** — Indicates that SNMP traps are sent to this host.

- **informs** — Indicates that SNMP informs are sent to this host.
- **noauth** — Indicates no authentication of a packet.
- **auth** — Indicates authentication of a packet without encrypting it.
- **priv** — Indicates authentication of a packet with encryption.
- *port* — Specifies the UDP port of the host to use. If unspecified, the default UDP port number is 162. (Range: 1-65535)
- *filtername*—Specifies a string that defines the filter for this host. If unspecified, nothing is filtered. (Range: 1-30 characters)
- *seconds* — Specifies the number of seconds to wait for an acknowledgment before resending informs. If unspecified, the default timeout period is **15** seconds. (Range: 1-300)
- *retries* — Specifies the maximum number of times to resend an inform request. If unspecified, the default maximum number of retries is **3**. (Range: 0-255)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

A user and notification view are not automatically created. Use the **snmp-server user**, **snmp-server group** and **snmp-server view** Global Configuration mode commands to generate a user, group and notify group, respectively.

Example

The following example configures an SNMPv3 host.

```
Console(config)# snmp-server v3-host 192.168.0.20 john noauth
```

snmp-server engineID local

The **snmp-server engineID local** Global Configuration mode command specifies the Simple Network Management Protocol (SNMP) engineID on the local device. Use the **no** form of this command to remove the configured engine ID.

Syntax

snmp-server engineID local {*engineid-string* | **default**}

no snmp-server engineID local

Parameters

- *engineid-string* — Specifies a character string that identifies the engine ID. (Range: 5-32 characters)
- **default** — The engine ID is created automatically based on the device MAC address.

Default Configuration

The engine ID is not configured.

If SNMPv3 is enabled using this command, and the default is specified, the default engine ID is defined per standard as:

- First 4 octets — first bit = 1, the rest is IANA Enterprise number = 674.
- Fifth octet — set to 3 to indicate the MAC address that follows.
- Last 6 octets — MAC address of the device.

Command Mode

Global Configuration mode

User Guidelines

To use SNMPv3, you have to specify an engine ID for the device. You can specify your own ID or use a default string that is generated using the MAC address of the device.

If the SNMPv3 engine ID is deleted or the configuration file is erased, SNMPv3 cannot be used. By default, SNMPv1/v2 are enabled on the device. SNMPv3 is enabled only by defining the Local Engine ID.

If you want to specify your own ID, you do not have to specify the entire 32-character engine ID if it contains trailing zeros. Specify only the portion of the engine ID up to the point where just zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can specify snmp-server engineID local 1234.

Since the engine ID should be unique within an administrative domain, the following is recommended:

Use the default keyword to configure the engine ID.

Changing the value of the engine ID has the following important side-effect. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The user's command line password is then destroyed, as required by RFC 2274. As a result, the security digests of SNMPv3 users become invalid if the local value of the engine ID change, and the users will have to be reconfigured.

You cannot specify an engine ID that consists of all 0x0, all 0xF or 0x000000001.

The **show running-config** Privileged EXEC mode command does not display the SNMP engine ID configuration. To see the SNMP engine ID configuration, enter the **snmp-server engineID local** Global Configuration mode command.

Example

The following example enables SNMPv3 on the device and sets the local engine ID of the device to the default value.

```
Console(config) # snmp-server engineID local default
```

snmp-server enable traps

The **snmp-server enable traps** Global Configuration mode command enables the device to send SNMP traps. Use the **no** form of this command to disable SNMP traps.

Syntax

snmp-server enable traps

no snmp-server enable traps

Default Configuration

SNMP traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables SNMP traps.

```
Console(config)# snmp-server enable traps
```

snmp-server trap authentication

The **snmp-server trap authentication** Global Configuration mode command enables the device to send SNMP traps when authentication fails. Use the **no** form of this command to disable SNMP failed authentication traps.

Syntax

snmp-server trap authentication

no snmp-server trap authentication

Default Configuration

SNMP failed authentication traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables SNMP failed authentication traps.

```
Console(config)# snmp-server trap authentication
```

snmp-server contact

The **snmp-server contact** Global Configuration mode command configures the system contact (sysContact) string. Use the **no** form of this command to remove system contact information.

Syntax

snmp-server contact *text*

no snmp-server contact

Parameters

- *text* — Specifies the string that describes system contact information. (Range: 1-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Do not include spaces in the text string or place text that includes spaces inside quotation marks.

Example

The following example configures the system contact point called **LinkSys_Technical_Support**

```
console(config)# snmp-server contact LinkSys_Technical_Support
```

snmp-server location

The **snmp-server location** Global Configuration mode command configures the system location string. Use the **no** form of this command to remove the location string.

Syntax

snmp-server location *text*

no snmp-server location

Parameters

- *text* — Specifies a string that describes system location information. (Range: 1-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Do not include spaces in the text string or place text that includes spaces inside quotation marks.

Example

The following example defines the device location as **New York**.

```
Console(config)# snmp-server location New_York
```

snmp-server set

The **snmp-server set** Global Configuration mode command defines the SNMP MIB value.

Syntax

snmp-server set *variable-name name1 value1* [*name2 value2* ...]

Parameters

- *variable-name* — MIB variable name (Range 1-160 characters).
- *name value* — List of name and value pairs. In the case of scalar MIBs, only a single pair of name values. In the case of an entry in a table, at least one pair of name and value followed by one or more fields (Range 1-160 characters).

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Although the CLI can set any required configuration, there might be a situation where a SNMP user sets a MIB variable that does not have an equivalent command. In order to generate configuration files that support those situations, the **snmp-server set** command is used.

This command is case-sensitive.

Example

The following example configures the scalar MIB sysName with the value **LinkSys**.

```
Console(config)# snmp-server set sysName sysname LinkSys
```

show snmp

The **show snmp** Privileged EXEC mode command displays the SNMP status.

Syntax

show snmp

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SNMP communications status.

```
Console# show snmp

Community-        Community-    View name     IP
String            Access                      address
----------        -----------   ---------     --------
public            read only     user-view     All
private           read write    Default       172.16.1.1
private           se            DefaultSuper  172.16.1.1


Community-string  Group name    IP address    Type
----------------  -----------   ---------
public            user-group    all
```

```
Traps are enabled.
Authentication trap is enabled.

Version 1,2 notifications

Target Address Type   Community Version UDP  Filter TO  Retries
                                        Port Name   Sec
-------------- -----  --------- ------- ---- ------ --- -------
192.122.173.42 Trap   Public    2       162         15  3
192.122.173.42 Inform Public    2       162         15  3


Version 3 Notifications

Target Address Type   Username Security UDP  Filter TO  Retries
                               Level    Port Name   Sec
-------------- -----  ---------------- ---- ------ --- -------
192.122.173.42 Inform Bob      Priv     162         15  3

System Contact: Robert
System Location: Marketing
```

The following table describes the significant fields shown in the display.

Field	Description
Community-string	Community access string to permit access to the SNMP protocol.
Community-access	Type of access - read-only, read-write, super access
IP Address	Management station IP Address.
Trap-Rec-Address	Targeted Recipient
Trap-Rec-Community	Statistics sent with the notification operation.
Version	SNMP version for the sent trap 1 or 2.

show snmp engineID

The **show snmp engineID** Privileged EXEC mode command displays the ID of the local Simple Network Management Protocol (SNMP) engine.

Syntax

show snmp engineID

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SNMP engine ID.

```
Console# show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
```

show snmp views

The **show snmp views** Privileged EXEC mode command displays the configuration of views.

Syntax

show snmp views [*viewname*]

Parameters

- *viewname* — Specifies the name of the view. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of views.

```
Console# show snmp views

Name       OID Tree               Type
---------- ------------------    --------
user-view  1.3.6.1.2.1.1         Included
user-view  1.3.6.1.2.1.1.7       Excluded
user-view  1.3.6.1.2.1.2.2.1.*.1 Included
```

show snmp groups

The **show snmp groups** Privileged EXEC mode command displays the configuration of groups.

Syntax

show snmp groups [*groupname*]

Parameters

- *groupname*—Specifies the name of the group. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of views.

```
Console# show snmp groups

Name                  Security               Views

                  Model  Level Read        Write    Notify
-------------     -----  ----- ----        -----    ------
user-group        V3     priv  Default              ""
managers-group    V3     priv  Default              ""
managers-group    V3     priv  Default    ""        ""
```

The following table describes significant fields shown above.

Field		Description
Name		Name of the group.
Security Mode		SNMP model in use (v1, v2 or v3).
Security Level		Authentication of a packet with encryption. Applicable only to SNMP v3 security.

Field		Description
Views	Read	Name of the view that enables only viewing the contents of the agent. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.
	Write	Name of the view that enables entering data and managing the contents of the agent.
	Notify	Name of the view that enables specifying an inform or a trap.

show snmp filters

The **show snmp filters** Privileged EXEC mode command displays the configuration of filters.

Syntax

show snmp filters [*filtername*]

Parameters

- *filtername* — Specifies the name of the filter. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of filters.

```
Console# show snmp filters

Name          OID Tree              Type
------------  -------------------   -----
user-filter   1.3.6.1.2.1.1         Included
user-filter   1.3.6.1.2.1.1.7       Excluded
user-filter   1.3.6.1.2.1.2.2.1.*.1 Included
```

show snmp users

The **show snmp users** Privileged EXEC mode command displays the configuration of users.

Syntax

show snmp users [*username*]

Parameters

- *username*—Specifies the name of the user. (Range: 1-30)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the configuration of users.

```
Console# show snmp users

Name     Group name    Auth Method   Remote
------   ------------  -----------   ---------------------
John     user-group    md5
John     user-group    md5           08009009020C0B099C075879
```

27

RSA and Certificate Commands

crypto certificate generate

The **crypto certificate generate** Global Configuration mode command generates a self-signed HTTPS certificate.

Syntax

crypto certificate [*number*] **generate** [**key-generate** *length*] [**cn** *common- name*] [**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*] [**duration** *days*]

Parameters

- *number* — Specifies the certificate number. (Range: 1-2)
- **key-generate** — Regenerate the SSL RSA key.
- *length* — Specifies the SSL RSA key length. (Range: 512-2048)
- *common- name* — Specifies the fully qualified URL or IP address of the device. (Range: 1-64)
- *organization-unit* — Specifies the organization-unit or department name.(Range: 1-64)
- *organization* — Specifies the organization name. (Range: 1-64)
- *location* — Specifies the location or city name. (Range: 1-64)
- *state* — Specifies the state or province name. (Range: 1-64)
- *country* — Specifies the country name. (Range: 2-2)
- *days* — Specifies number of days certification is valid. (Range: 30-3650)

Default Configuration

The Certificate and SSL's RSA key pairs do not exist.

If no RSA key length is specified, the default length is 1024.

If no URL or IP address is specified, the default common name is the lowest IP address of the device at the time that the certificate is generated.

If the number of days is not specified, the default period of time that the certification is valid is 365 days.

Command Mode

Global Configuration mode

User Guidelines

The command is not saved in the device configuration; however, the certificate and keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

Use this command to generate a self-signed certificate for the device.

If the RSA keys do not exist, parameter **key-generate** must be used.

Example

The following example regenerates an HTTPS certificate.

```
Console(config)# crypto certificate 1 generate key-generate
```

crypto key generate dsa

The **crypto key generate dsa** Global Configuration mode command generates DSA key pairs.

Syntax

crypto key generate dsa

Default Configuration

DSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

DSA keys are generated in pairs: one public DSA key and one private DSA key. If the device already has DSA keys, a warning and prompt to replace the existing keys with new keys are displayed.

This command is not saved in the device configuration; however, the keys generated by this command are saved in the private configuration, which is never displayed to the user or backed up on another device.

This command may take a considerable period of time to execute.

Example

The following example generates DSA key pairs.

```
Console(config)# crypto key generate dsa
```

crypto key generate rsa

The **crypto key generate rsa** Global Configuration mode command generates RSA key pairs.

Syntax

crypto key generate rsa

Default Configuration

RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

RSA keys are generated in pairs: one public RSA key and one private RSA key. If the device already has RSA keys, a warning and prompt to replace the existing keys with new keys are displayed.

This command is not saved in the device configuration; however, the keys generated by this command are saved in the private configuration which is never displayed to the user or backed up on another device.

This command may take a considerable period of time to execute.

Example

The following example generates RSA key pairs.

```
Console(config)# crypto key generate rsa
```

28

Spanning Tree Commands

spanning-tree

The **spanning-tree** Global Configuration mode command enables spanning-tree functionality. Use the **no** form of this command to disable the spanning-tree functionality.

Syntax

spanning-tree

no spanning-tree

Default Configuration

Spanning-tree is enabled.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables spanning-tree functionality.

```
Console(config)# spanning-tree
```

spanning-tree mode

The **spanning-tree mode** Global Configuration mode command configures the spanning-tree protocol. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mode {**stp** | **rstp** | **mstp**}

no spanning-tree mode

Parameters

- **stp** — Indicates that the Spanning Tree Protocol (STP) is enabled.
- **rstp** — Indicates that the Rapid Spanning Tree Protocol (RSTP) is enabled.
- **mstp** — Indicates that the Multiple Spanning Tree Protocol (RSTP) is enabled.

Default Configuration

STP is enabled.

Command Modes

Global Configuration mode

User Guidelines

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP and uses STP when the neighbor device uses STP.

Example

The following example configures the spanning-tree protocol to RSTP.

```
console(config)# spanning-tree mode rstp
```

spanning-tree forward-time

The **spanning-tree forward-time** Global Configuration mode command configures the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

Parameters

- *seconds* **—** Time in seconds. (Range: 4-30)

Default Configuration

The default forwarding time for the IEEE Spanning Tree Protocol (STP) is **15** seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the forwarding time, the following relationship should be kept:

2*(Forward-Time - 1) >= Max-Age

Example

The following example configures the spanning tree bridge forwarding time to 25 seconds.

```
Console(config)# spanning-tree forward-time 25
```

spanning-tree hello-time

The **spanning-tree hello-time** Global Configuration mode command configures the spanning tree bridge hello time, which is how often the device Broadcasts hello messages to other devices. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree hello-time *seconds*

no spanning-tree hello-time

Parameters

- *seconds* — Time in seconds. (Range: 1-10)

Default Configuration

The default hello time for IEEE Spanning Tree Protocol (STP) is **2** seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the hello time, the following relationship should be kept:

Max-Age >= 2*(Hello-Time + 1)

Example

The following example configures spanning tree bridge hello time to 5 seconds.

```
Console(config)# spanning-tree hello-time 5
```

spanning-tree max-age

The **spanning-tree max-age** Global Configuration mode command configures the spanning tree bridge maximum age. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

Parameters

- *seconds* — Time in seconds. (Range: 6-40)

Default Configuration

The default maximum age for IEEE Spanning Tree Protocol (STP) is **20** seconds.

Command Modes

Global Configuration mode

User Guidelines

When configuring the maximum age, the following relationships should be kept:

2*(Forward-Time - 1) >= Max-Age

Max-Age >= 2*(Hello-Time + 1)

Example

The following example configures the spanning tree bridge maximum-age to 10 seconds.

```
Console(config)# spanning-tree max-age 10
```

spanning-tree priority

The **spanning-tree priority** Global Configuration mode command configures the spanning tree priority of the device. The priority value is used to determine which bridge is elected as the root bridge. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

Parameters

- *priority* — Priority of the bridge. (Range: 0-61440 in steps of 4096)

Default Configuration

The default bridge priority for IEEE Spanning Tree Protocol (STP) is **32768**.

Command Modes

Global Configuration mode

User Guidelines

The bridge with the lowest priority is elected as the root bridge.

Example

The following example configures spanning tree priority to 12288.

```
Console(config)# spanning-tree priority 12288
```

spanning-tree disable

The **spanning-tree disable** Interface Configuration mode command disables spanning tree on a specific port. Use the **no** form of this command to enable spanning tree on a port.

Syntax

spanning-tree disable

no spanning-tree disable

Default Configuration

Spanning tree is enabled on all ports.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables spanning-tree on Ethernet port e5.

```
Console(config)# interface ethernet e5
Console(config-if)# spanning-tree disable
```

spanning-tree cost

The **spanning-tree cost** Interface Configuration mode command configures the spanning tree path cost for a port. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

Parameters

- *cost* — Path cost of the port (Range: 1-200,000,000)

Default Configuration

Default path cost is determined by port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The path cost method is configured using the **spanning-tree pathcost method** Global Configuration mode command.

Example

The following example configures the spanning-tree cost on Ethernet port e15 to 35000.

```
Console(config)# interface ethernet e15
```

```
Console(config-if)# spanning-tree cost 35000
```

spanning-tree port-priority

The **spanning-tree port-priority** Interface Configuration mode command configures port priority. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

Parameters

- *priority* — The priority of the port. (Range: 0-240 in multiples of 16)

Default Configuration

The default port priority for IEEE Spanning TreeProtocol (STP) is **128**.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the spanning priority on Ethernet port e15 to 96.

```
Console(config)# interface ethernet e15
Console(config-if)# spanning-tree port-priority 96
```

spanning-tree portfast

The **spanning-tree portfast** Interface Configuration mode command enables PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup without waiting for the standard forward time delay. Use the **no** form of this command to disable PortFast mode.

Syntax

spanning-tree portfast [**auto**]

no spanning-tree portfast

Parameters

- **auto —** Specifies that the software waits for 3 seconds (With no BPDUs received on the interface) before putting the interface into the PortFast mode.

Default Configuration

PortFast mode is enabled.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This feature should be used only with interfaces connected to end stations. Otherwise, an accidental topology loop could cause a data packet loop and disrupt device and network operations.

Example

The following example enables PortFast on Ethernet port e15.

```
Console(config)# interface ethernet e15

Console(config-if)# spanning-tree portfast
```

spanning-tree link-type

The **spanning-tree link-type** Interface Configuration mode command overrides the default link-type setting determined by the duplex mode of the port and enables Rapid Spanning Tree Protocol (RSTP) transitions to the forwarding state. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree link-type

Parameters

- **point-to-point** —Indicates that the port link type is point-to-point.
- **shared** — Indicates that the port link type is shared.

Default Configuration

The device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables shared spanning-tree on Ethernet port e5.

```
Console(config)# interface ethernet e15
Console(config-if)# spanning-tree link-type shared
```

spanning-tree pathcost method

The **spanning-tree pathcost method** Global Configuration mode command sets the default path cost method. Use the **no** form of this command to return to the default configuration.

Syntax

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

Parameters

- **long** — Specifies port path costs with a range of 1-200,000,000.
- **short** — Specifies port path costs with a range of 0-65,535.

Default Configuration

Short path cost method.

Command Mode

Global Configuration mode

User Guidelines

This command is only operational with the device in Interface mode.

This command applies to all spanning tree instances on the device.

The cost is set using the **spanning-tree** cost command.

Example

The following example sets the default path cost method to **long**.

```
Console(config)# spanning-tree pathcost method long
```

spanning-tree bpdu

The **spanning-tree bpdu** Global Configuration mode command defines BPDU handling when the spanning tree is disabled globally or on a single interface. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree bpdu {**filtering** | **flooding** | **bridging**}

no spanning-tree bpdu

Parameters

- **filtering** — Filter BPDU packets when the spanning tree is disabled on an interface.
- **flooding** — Flood BPDU packets when the spanning tree is disabled on an interface.

- **bridging** — Bridge BPDU packets when spanning tree is disabled globally, untagged or tagged frames are flooded and are subject to ingress and egress VLAN rules

Default Configuration

The default setting is flooding.

Command Modes

Global Configuration mode

User Guidelines

The filtering and flooding modes are relevant when spanning-tree is disabled globally or on a single interface.

Example

The following example defines BPDU packet flooding when the spanning-tree is disabled on an interface.

```
Console(config)# spanning-tree bpdu flooding
```

spanning-tree guard root

The **spanning-tree guard root** Interface Configuration (Ethernet, port-channel) mode command enables root guard on all spanning tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. Use the **no** form of this command to disable root guard on the interface.

Syntax

spanning-tree guard root

no spanning-tree guard root

Default Configuration

Root guard is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

Root guard can be enabled when the device operates in STP, RSTP and MSTP.

When root guard is enabled, the port changes to the alternate state if spanning-tree calculations selects the port as the root port.

Example

The following example prevents Ethernet port e1 from being the root port of the device.

```
Console(config) # interface ethernet e1

Console(config-mst) # spanning-tree guard root
```

clear spanning-tree detected-protocols

The **clear spanning-tree detected-protocols** Privileged EXEC mode command restarts the protocol migration process (forces renegotiation with neighboring devices) on all interfaces or on a specified interface.

Syntax

clear spanning-tree detected-protocols [**ethernet** *interface* | **port-channel** *port-channel-number*]

Parameters

- *interface* — A valid Ethernet port.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

This feature should be used only when working in RSTP or MSTP mode.

Example

The following example restarts the protocol migration process on Ethernet port e11.

```
Console# clear spanning-tree detected-protocols ethernet e11
```

spanning-tree mst priority

The **spanning-tree mst priority** Global Configuration mode command configures the device priority for the specified spanning-tree instance. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

Parameters

- *instance-id*—ID of the spanning-tree instance (Range: 1-7).
- *priority*—Device priority for the specified spanning-tree instance (Range: 0-61440 in multiples of 4096).

Default Configuration

The default bridge priority for IEEE Spanning Tree Protocol (STP) is **32768**.

Command Mode

Global Configuration mode

User Guidelines

The device with the lowest priority is selected as the root of the spanning tree.

Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
Console (config) # spanning-tree mst 1 priority 4096
```

spanning-tree mst max-hops

The **spanning-tree mst priority** Global Configuration mode command configures the number of hops in an MST region before the BDPU is discarded and the port information is aged out. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Parameters

- *hop-count*—Number of hops in an MST region before the BDPU is discarded. (Range: 1-40)

Default Configuration

The default number of hops is 20.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
Console (config) # spanning-tree mst max-hops 10
```

spanning-tree mst port-priority

The **spanning-tree mst port-priority** Interface Configuration mode command configures port priority for the specified MST instance. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

Parameters

- *instance-ID*—ID of the spanning tree instance. (Range: 1-7)
- *priority*—The port priority. (Range: 0-240 in multiples of 16)

Default Configuration

The default port priority for IEEE Multiple Spanning Tree Protocol (MSTP) is **128**.

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the port priority of port g1 to 144.

```
Console(config)# interface ethernet g1
Console(config-if)# spanning-tree mst 1 port-priority 144
```

spanning-tree mst cost

The **spanning-tree mst cost** Interface Configuration mode command configures the path cost for multiple spanning tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

Parameters

- *instance-ID*—ID of the spanning-tree instance (Range: 1-7).
- *cost*—The port path cost. (Range: 1-200,000,000)

Default Configuration

Default path cost is determined by port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Modes

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the MSTP instance 1 path cost for Ethernet port e9 to 4.

```
Console(config) # interface ethernet e9
Console(config-if) # spanning-tree mst 1 cost 4
```

spanning-tree mst configuration

The **spanning-tree mst configuration** Global Configuration mode command enables configuring an MST region by entering the Multiple Spanning Tree (MST) mode.

Syntax

spanning-tree mst configuration

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

All devices in an MST region must have the same VLAN mapping, configuration revision number and name.

Example

The following example configures an MST region.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)#
```

instance (mst)

The **instance** MST Configuration mode command maps VLANS to an MST instance.

Syntax

instance *instance-id* {**add** | **remove**} **vlan** *vlan-range*

Parameters

- *instance-ID*—ID of the MST instance (Range: 1- 7).
- *vlan-range*—VLANs to be added to or removed from the specified MST instance. To specify a range of VLANs, use a hyphen. To specify a series of VLANs, use a comma. (Range: 1-4094).

Default Configuration

VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Modes

MST Configuration mode

User Guidelines

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 1 add vlan 10-20
```

name (mst)

The **name** MST Configuration mode command defines the configuration name. Use the **no** form of this command to restore the default setting.

Syntax

name *string*

Parameters

- *string* — MST configuration name. The name is case-sensitive. (Range: 1-32 characters)

Default Configuration

The default name is a radlan_guest.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example defines the configuration name as region1.

```
Console(config) # spanning-tree mst_configuration
Console(config-mst) # name region1
```

revision (mst)

The **revision** MST Configuration mode command defines the configuration revision number. Use the **no** form of this command to restore the default configuration.

Syntax

revision *value*

no revision

Parameters

- *value* — Configuration revision number (Range: 0-65535).

Default Configuration

The default configuration revision number is **0**.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the configuration revision to 1.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # revision 1
```

show (mst)

The **show** MST Configuration mode command displays the current or pending MST region configuration.

Syntax

show {**current** | **pending**}

Parameters

- **current**—Indicates the current region configuration.
- **pending**—Indicates the pending region configuration.

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

The pending MST region configuration takes effect only after exiting the MST Configuration mode.

Example

The following example displays a pending MST region configuration.

```
Console(config-mst)# show pending
Pending MST configuration
Name: Region1
Revision: 1
Instance  VLANs Mapped     State
0         1-9,21-4094      Enabled
1         10-20            Enabled
```

exit (mst)

The **exit** MST Configuration mode command exits the MST Configuration mode, and applies all configuration changes.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example exits the MST Configuration mode and saves changes.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # exit
Console(config) #
```

abort (mst)

The **abort** MST Configuration mode command exits the MST Configuration mode without applying the configuration changes.

Syntax

abort

Default Configuration

This command has no default configuration.

Command Mode

MST Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example exits the MST Configuration mode without saving changes.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # abort
```

show spanning-tree

The **show spanning-tree** Privileged EXEC mode command displays spanning-tree configuration.

Syntax

show spanning-tree [**ethernet** *interface -number*| **port-channel** *port-channel-number*] [**instance** *instance-id*]

show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *instance-id*]

how spanning-tree mst-configuration

Parameters

- *interface -number* — A valid Ethernet port.
- *port-channel-number* — A valid port channel number.
- **detail** — Indicates detailed information.
- **active** — Indicates active ports only.
- **blockedports** — Indicates blocked ports only.
- **mst-configuration** — Indicates the MST configuration identifier.
- *instance-id* —Specifies ID of the spanning tree instance. (Range: 1-7)

Default Configuration

This command has no default configuration.

Command Modes

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays spanning-tree information.

Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: short

```
CST Root ID  Priority       32768
             Address        00:01:42:97:e0:00
             Path Cost      20000
             Root Port      1 (e1)
             This switch is the IST master
             Hello Time 2 sec Max Age 20 sec  Forward Delay 15 sec

Bridge ID Priority                             36864
             Address        00:02:4b:29:7a:00
             Hello Time 2 sec Max Age 20 sec  Forward Delay 15 sec
                            Max Hops           20

Interfaces
Name  State    Pro.Nbr  Cost   Sts  Role  PortFast Type
----  -------- -------- -----  ---  ----  -------- ----------
e1    Enabled 128.1     20000  FWD  Root  No       P2p bound (RSTP)
e2    Enabled 128.2     20000  FWD  Desg  No       Shared (STP)
e3    Disabled128.3     20000  -    -     -        -
e4    Enabled 128.4     20000  BLK  ALTN  No       Shared (STP)
e5    Enabled 128.5     20000  DIS  -     -        -


Console# show spanning-tree

Spanning tree enabled mode RSTP
Default port cost method:  long

Root ID     Priority        36864
             Address        00:02:4b:29:7a:00
             This switch is the root.
             Hello Time 2 sec Max Age 20 sec  Forward Delay 15 sec

Interfaces
```

```
Name State    Prio.Nbr Cost  Sts Role PortFast Type
---- -------  -------- ----- --- ---- -------- ----------
e1   Enabled  128.1    20000 FWD Desg No       P2p (RSTP)
e2   Enabled  128.2    20000 FWD Desg No       Shared (STP)
e3   Disabled 128.3    20000 -   -    -        -
e4   Enabled  128.4    20000 FWD Desg No       Shared (STP)
e5   Enabled  128.5    20000 DIS -    -        -


Console# show spanning-tree

Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long

Root ID   Priority         N/A
          Address          N/A
          Path Cost        N/A
          Root Port        N/A
          Hello Time N/A   Max Age N/A     Forward Delay N/A

Bridge ID Priority         36864
          Address          00:02:4b:29:7a:00
          Hello Time 2 sec Max Age 20 sec  Forward Delay 15 sec

Interfaces
Name State   Prio.Nbr Cost  Sts Role PortFast Type
---- ------- -------- ----- --- ---- -------- ----
e1   Enabled 128.1    20000 -    -    -        -
e2   Enabled 128.2    20000 -    -    -        -
e3   Disabled128.3    20000 -    -    -        -
e4   Enabled 128.4    20000 -    -    -        -
e5   Enabled 128.5    20000 -    -    -        -


Console# show spanning-tree active

Spanning tree enabled mode RSTP
Default port cost method: long
```

```
Root ID   Priority         32768
          Address          00:01:42:97:e0:00
          Path Cost        20000
          Root Port        1 (e1)
          Hello Time 2 sec Max Age 20 sec  Forward Delay 15 sec

Bridge ID    Priority      36864
          Address          00:02:4b:29:7a:00
          Hello Time 2 sec Max Age 20 sec  Forward Delay 15 sec

Interfaces
Name State   Prio.Nbr Cost  Sts  Role  PortFast Type
---- ------- -------- ----- ---  ----  -------- ----------
e1   Enabled 128.1    20000 FWD  Root  No       P2p (RSTP)
e2   Enabled 128.2    20000 FWD  Desg  No       Shared (STP)
e4   Enabled 128.4    20000 BLK  ALTN  No       Shared (STP)


Console# show spanning-tree blockedports

Spanning tree enabled mode RSTP
Default port cost method:  long

Root ID   Priority         32768
          Address          00:01:42:97:e0:00
          Path Cost        20000
          Root Port        1 (e1)
          Hello Time 2 sec Max Age 20 sec  Forward Delay 15 sec

Bridge ID Priority         36864
          Address          00:02:4b:29:7a:00
          Hello Time 2 sec Max Age 20 sec  Forward Delay 15 sec

Interfaces
Name State   Prio.Nbr Cost  Sts  Role  PortFast Type
---- ------- -------- ----- ---  ----  -------- ----------
e4   Enabled 128.4    20000 BLK  ALTN  No       Shared (STP)


Console# show spanning-tree detail

Spanning tree enabled mode RSTP
Default port cost method:  long
```

```
Root ID   Priority         32768
          Address          00:01:42:97:e0:00
          Path Cost        20000
          Root Port        1 (e1)
          Hello Time 2 sec Max Age 20 sec  Forward Delay 15 sec

Bridge ID Priority         36864
          Address          00:02:4b:29:7a:00
          Hello Time 2 sec Max Age 20 sec  Forward Delay 15 sec

Number of topology changes 2 last change occurred 2d18h ago
Times:    hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15

Port 1 (e1) enabled
State: Forwarding          Role: Root
Port id: 128.1             Port cost: 20000
Type: P2p (configured: auto) RSTPPort Fast: No (configured:no)
Designated bridge Priority: 32768Address: 00:01:42:97:e0:00
Designated port id: 128.25 Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (e2) enabled
State: Forwarding          Role: Designated
Port id: 128.2             Port cost: 20000
Type: Shared (configured: auto) STPPort Fast: No
(configured:no)
Designated bridge Priority: 32768Address: 00:02:4b:29:7a:00
Designated port id: 128.2  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (e3) disabled
State: N/A                 Role: N/A
Port id: 128.3             Port cost: 20000
Type: N/A (configured: auto) Port Fast: N/A (configured:no)
Designated bridge Priority: N/AAddress: N/A
Designated port id: N/A    Designated path cost: N/A
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A
```

```
Port 4 (e4) enabled
State: Blocking              Role: Alternate
Port id: 128.4               Port cost: 20000
Type: Shared (configured:auto) STPPort Fast: No (configured:no)
Designated bridge Priority: 28672Address: 00:30:94:41:62:c8
Designated port id: 128.25 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 5 (e5) enabled
State: Disabled              Role: N/A
Port id: 128.5               Port cost: 20000
Type: N/A (configured: auto) Port Fast: N/A (configured:no)
Designated bridge Priority: N/AAddress: N/A
Designated port id: N/A      Designated path cost: N/A
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A


Console# show spanning-tree ethernet e1

Port 1 (e1) enabled
State: Forwarding            Role: Root
Port id: 128.1               Port cost: 20000
Type: P2p (configured: auto) RSTPPort Fast: No (configured no)
Designated bridge Priority: 32768Address: 00:01:42:97:e0:00
Designated port id: 128.25 Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Console# show spanning-tree mst-configuration

Name: Region1
Revision: 1

Instance  Vlans mapped     State
--------  ------------     -------
0         1-9, 21-4094     Enabled
1         10-20            Enabled


Console# show spanning-tree
```

```
Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9, 21-4094
CST Root ID Priority        32768
            Address         00:01:42:97:e0:00
            Path Cost       20000
            Root Port       1 (e1)
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

IST Master IDPriority       32768
            Address         00:02:4b:29:7a:00
            This switch is the IST master.
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
            Max hops        20

Interfaces
Name State    Prio.Nbr Cost  Sts Role PortFast Type
---- -------- -------- ----- --- ---- -------- ----------
e1   Enabled  128.1    20000 FWD Root No       P2p Bound (RSTP)
e2   Enabled  128.2    20000 FWD Desg No       Shared Bound (STP)
e3   Enabled  128.3    20000 FWD Desg No       P2p
e4   Enabled  128.4    20000 FWD Desg No       P2p

###### MST 1 Vlans Mapped: 10-20
CST Root IDPriority       24576
           Address        00:02:4b:29:89:76
           Path Cost      20000
           Root Port      4 (e4)
           Rem hops       19

Bridge ID  Priority       32768
           Address        00:02:4b:29:7a:00

Interfaces
Name State    Prio.Nbr Cost  Sts Role PortFast Type
---- -------- -------- ----- --- ---- -------- ----------
e1   Enabled  128.1    20000 FWD Boun No       P2p Bound (RSTP)
e2   Enabled  128.2    20000 FWD Boun No       Shared Bound (STP)
e3   Enabled  128.3    20000 BLK Altn No       P2p
e4   Enabled  128.4    20000 FWD Desg No       P2p
```

```
Console# show spanning-tree detail


Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9, 21-4094
CST Root ID Priority        32768
            Address         00:01:42:97:e0:00
            Path Cost       20000
            Root Port       1 (e1)
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

IST Master IDPriority32768
            Address00:02:4b:29:7a:00
            This switch is the IST master.
            Hello Time 2 secMax Age 20 secForward Delay 15 sec
            Max hops 20
            Number of topology changes 2 last change occurred 2d18h ago
            Times:  hold 1, topology change 35, notification 2
            hello 2, max age 20, forward delay 15

Port 1 (e1) enabled
State: Forwarding          Role: Root
Port id: 128.1             Port cost: 20000
Type: P2p (configured: auto) Boundary RSTPPort Fast: No
(configured:no)
Designated bridge Priority: 32768Address: 00:01:42:97:e0:00
Designated port id: 128.25 Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (e2) enabled
State: Forwarding          Role: Designated
Port id: 128.2             Port cost: 20000
Type: Shared (configured: auto) Boundary STPPort Fast: No
(configured:no)
Designated bridge Priority: 32768Address: 00:02:4b:29:7a:00
Designated port id: 128.2  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
```

```
Port 3 (e3) enabled
State: Forwarding         Role: Designated
Port id: 128.3            Port cost: 20000
Type: Shared (configured: auto) InternalPort Fast: No
(configured:no)
Designated bridge Priority: 32768Address: 00:02:4b:29:7a:00
Designated port id: 128.3 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 4 (e4) enabled
State: Forwarding         Role: Designated
Port id: 128.4            Port cost: 20000
Type: Shared (configured: auto) InternalPort Fast: No
(configured:no)
Designated bridge Priority: 32768Address: 00:02:4b:29:7a:00
Designated port id: 128.2 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


###### MST 1 Vlans Mapped: 10-20
Root ID   Priority        24576
          Address         00:02:4b:29:89:76
          Path Cost       20000
          Port Cost       4 (e4)
          Rem hops        19

Bridge ID Priority        32768
          Address         00:02:4b:29:7a:00
          Number of topology changes 2 last change occurred 1d9h ago
          Times:  hold 1, topology change 2, notification 2
          hello 2, max age 20, forward delay 15

Port 1 (e1) enabled
State: Forwarding         Role: Boundary
Port id: 128.1            Port cost: 20000
Type: P2p (configured: auto) Boundary RSTPPort Fast: No
```

```
(configured:no)
Designated bridge Priority: 32768Address: 00:02:4b:29:7a:00
Designated port id: 128.1  Designated path cost: 20000

Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (e2) enabled
State: Forwarding           Role: Designated
Port id: 128.2              Port cost: 20000
Type: Shared (configured: auto) Boundary STPPort Fast: No
(configured:no)
Designated bridge Priority: 32768Address: 00:02:4b:29:7a:00
Designated port id: 128.2  Designated path cost: 20000 Number
of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (e3) disabled
State: Blocking             Role: Alternate
Port id: 128.3              Port cost: 20000
Type: Shared (configured: auto) InternalPort Fast: No
(configured:no)
Designated bridge Priority: 32768Address: 00:02:4b:29:1a:19
Designated port id: 128.78  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 4 (e4) enabled
State: Forwarding           Role: Designated
Port id: 128.4              Port cost: 20000
Type: Shared (configured: auto) InternalPort Fast: No
(configured:no)
Designated bridge Priority: 32768Address: 00:02:4b:29:7a:00
Designated port id: 128.2  Designated path cost: 20000 Number
of transitions to forwarding state: 1
BPDU: sent 2, received 170638
```

```
Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9, 21-4094
CST Root ID   Priority        32768
              Address         00:01:42:97:e0:00
              Path Cost       20000
              Root Port       1 (e1)
              Hello Time 2 sec Max Age 20 secForward Delay 15 sec


IST Master ID Priority        32768
              Address         00:02:4b:19:7a:00
              Path Cost       10000
              Rem hops        19

Bridge ID     Priority        32768
              Address         00:02:4b:29:7a:00
              Hello Time 2 sec Max Age 20 secForward Delay 15 sec
              Max hops        20


Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9, 21-4094
CST Root IDPriority          32768
           Address           00:01:42:97:e0:00
           This switch is root for CST and IST master.
           Root Port         1 (e1)
           Hello Time 2 sec  Max Age 20 sec Forward Delay 15 sec
           Max hops          20
```

29

SSH Commands

ip ssh port

The **ip ssh port** Global Configuration mode command specifies the port to be used by the SSH server. Use the **no** form of this command to restore the default configuration.

Syntax

ip ssh port *port-number*

no ip ssh port

Parameters

- *port-number* — Port number for use by the SSH server (Range: 1-65535).

Default Configuration

The default port number is **22**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the port to be used by the SSH server as 8080.

```
Console(config)# ip ssh port 8080
```

ip ssh server

The **ip ssh server** Global Configuration mode command enables the device to be configured from a SSH server. Use the **no** form of this command to disable this function.

Syntax

ip ssh server

no ip ssh server

Default Configuration

Device configuration from a SSH server is enabled.

Command Mode

Global Configuration mode

User Guidelines

If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the **crypto key generate dsa**, and **crypto key generate rsa** Global Configuration mode commands.

Example

The following example enables configuring the device from a SSH server.

```
Console(config)# ip ssh server
```

ip ssh pubkey-auth

The **ip ssh pubkey-auth** Global Configuration mode command enables public key authentication for incoming SSH sessions. Use the **no** form of this command to disable this function.

Syntax

ip ssh pubkey-auth

no ip ssh pubkey-auth

Default Configuration

Public Key authentication to incoming SSH sessions is disabled.

Command Mode

Global Configuration mode

User Guidelines

AAA authentication is independent.

Example

The following example enables public key authentication for incoming SSH sessions.

```
Console(config)# ip ssh pubkey-auth
```

crypto key pubkey-chain ssh

The **crypto key pubkey-chain ssh** Global Configuration mode command enters the SSH Public Key-chain Configuration mode. The mode is used to manually specify other device public keys such as SSH client public keys.

Syntax

crypto key pubkey-chain ssh

Default Configuration

No keys are specified.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enter public key chain configuration mode. Use this command when you need to manually specify SSH client's public keys.

Example

The following example enters the SSH Public Key-chain Configuration mode and manually configures the RSA key pair for SSH public key-chain **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob
Console(config-pubkey-key)# key-string rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
```

```
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

user-key

The **user-key** SSH Public Key-string Configuration mode command specifies which SSH public key is manually configured. Use the **no** form of this command to remove an SSH public key.

Syntax

user-key *username* {**rsa** | **dsa**}

no user-key *username*

Parameters

- *username* — Specifies the username of the remote SSH client. (Range: 1-48 characters)
- **rsa** — Indicates the RSA key pair.
- **dsa** — Indicates the DSA key pair.

Default Configuration

No SSH public keys exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

Follow this command with the **key-string** SSH Public Key-String Configuration mode command to specify the key.

Example

The following example enables manually configuring an SSH public key for SSH public key-chain **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
```

key-string

The **key-string** SSH Public Key-string Configuration mode command manually specifies an SSH public key.

Syntax

key-string

key-string row *key-string*

Parameters

- **row** — Indicates the SSH public key row by row.
- *key-string* — Specifies the key in UU-encoded DER format; UU-encoded DER format is the same format in the authorized_keys file used by OpenSSH. (Range:0-160)

Default Configuration

No keys exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

Use the **key-string** SSH Public Key-string Configuration mode command to specify which SSH public key is to be interactively configured next. To complete the command, you must enter a row with no characters.

Use the **key-string** row SSH Public Key-string Configuration mode command to specify the SSH public key row by row. Each row must begin with a **key-string row** command. This command is useful for configuration files.

UU-encoded DER format is the same format in authorized_keys file used by OpenSSH.

Example

The following example enters public key strings for SSH public key client **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9

Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row AAAAB3Nza
Console(config-pubkey-key)# key-string row C1yc2
```

show ip ssh

The **show ip ssh** Privileged EXEC mode command displays the SSH server configuration.

Syntax

show ip ssh

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the SSH server configuration.

```
Console# show ip ssh

SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.

SSH Public Key Authentication is enabled.

Active incoming sessions:

IP AddressSSH Username        Version   CipherAuth Code
172.16.0.1John Brown          2.0 3     DESHMAC-SHA1
```

The following table describes the significant fields shown in the display.

Field	Description
IP address	Client address
SSH Username	User name
Version	SSH version number
`	Encryption type (3DES, Blowfish, RC4)
Auth Code	Authentication Code (HMAC-MD5, HMAC-SHA1)

show crypto key pubkey-chain ssh

The **show crypto key pubkey-chain ssh** Privileged EXEC mode command displays SSH public keys stored on the device.

Syntax

show crypto key pubkey-chain ssh [**username** *username*] [**fingerprint** {**bubble-babble** | **hex**}]

Parameters

- *username* — Specifies the remote SSH client username.
- **bubble-babble** — Fingerprint in Bubble Babble format.
- **hex** — Fingerprint in Hex format.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays SSH public keys stored on the device.

```
Console# show crypto key pubkey-chain ssh

Username  Fingerprint
bob       9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
john      98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8

Console# show crypto key pubkey-chain ssh username bob

Username: bob

Key: 005C300D 06092A86 4886F70D 01010105 00034B00 30480241
00C5E23B 55D6AB22 04AEF1BA A54028A6 9ACC01C5 129D99E4

Fingerprint: 9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
```

show crypto key mypubkey

To view the SSH public keys of your device, use the **show crypto key mypubkey** Privileged EXEC command.

Syntax

show crypto key mypubkey [rsa | dsa]

Parameters

- **rsa** — RSA key
- **dsa** — DSA key

Default Configuration

This command has no default setting.

Command Mode

Privileged EXEC

Example

```
Console# show crypto key mypubkey rsa

RSA key data:

005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B
55D6AB22

04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C
73A05DD2

BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301
87685768

Fingerprint(Hex):
77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86

Fingerprint(Bubble Babble): yteriuwt jgkljhglk yewiury hdskjfryt
gfhkjglk
```

crypto certificate request

To generate and display certificate request for HTTPS, use the crypto certificate request command in privileged EXEC mode.

Syntax

crypto certificate *number* **request** *common- name* [**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*]

Parameters

- *number* — Specifies the certificate number. Range: 1 - 2 digits
- *common- name* — Specifies the fully qualified URL or IP address of the device. Range: 1 - 64 characters

- **ou** *organization-unit* — Specifies the organization-unit or department name. Range: 1 - 64 characters
- **or** *organization* — Specifies the organization name. Range: 1 - 64 characters
- **loc** *location* — Specifies the location or city name. Range: 1 - 64 characters
- **st** *state* — Specifies the state or province name. Range: 1 - 64 characters
- **cu** *country* — Specifies the country name. Range: 2 letters

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request you must first generate a self-signed certificate using the **crypto certificate generate** global configuration command in order to generate the keys. Be aware that you should reenter the certificates fields.

After receiving the certificate from the Certification Authority, use the **crypto certificate import** global configuration 1command to import the certificate into the device. This certificate would replace the self-signed certificate.

Examples

```
Console# crypto certificate 1 request

-----BEGIN CERTIFICATE REQUEST-----

MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAxCzAJBgNVBAgTAkNDMQswCQYDVQQH

EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
```

```
DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ

HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K

aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm

/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH

MRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBBAUAA4GBAGb8UgIx7rB05m+2

m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa

g+uNpyTkDt3ZVU72pjz/fa8TF0n3

-----END CERTIFICATE REQUEST-----


CN= router.gm.com

0= General Motors

C= US
```

crypto certificate import

To import a certificate signed by Certification Authority for HTTPS, use the crypto certificate import command in global configuration mode.

Syntax

crypto certificate *number* **import**

Parameters

- number — Specifies the certificate number. Range: 1 - 2 digits

Default Configuration

There is no default configuration for this command.

Command Mode

Global configuration

User Guidelines

Use this command to enter an external certificate (signed by Certification Authority) to the device. To end the session, use a blank line.

The imported certificate must be based on a certificate request created by the crypto certificate request privileged EXEC command.

If the public key found in the certificate does not match the device's SSL RSA key, the command will fail.

This command is not saved in the router configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).

Examples

```
Console(config)# crypto certificate 1 import
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----

Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
```

```
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

crypto certificate export

To export the certificate and the RSA keys, use the crypto certificate export command in Privileged EXEC mode.

Syntax

crypto certificate *number* **export**

Parameters

- *number* — Specifies the certificate number. Range: 1 - 2 digits

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC

User Guidelines

The **crypto certificate export** command creates a file that contains the certificate and an RSA key pair.

The passphrase for the exporting is determined when the key is generated.

Examples

```
Console# crypto certificate 1 export
```

show crypto certificate mycertificate

To view the SSL certificates of your device, use the show crypto certificate mycertificate Privileged EXEC command.

Syntax

show crypto certificate mycertificate [*number*]

Parameters

- *number* — Specifies the certificate number. Range: 1, product specific

Default value

This command has no default setting.

Command Mode

Privileged EXEC

Example

```
Console# show crypto certificate mycertificate 1
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----
```

```
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

30

Syslog Commands

logging on

The **logging on** Global Configuration mode command controls error message logging. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the process that generated the messages. Use the **no** form of this command to disable the logging process.

Syntax

logging on

no logging on

Default Configuration

Logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

The logging process controls the distribution of logging messages at various destinations, such as the logging buffer, logging file or syslog server. Logging on and off at these destinations can be individually configured using the **logging buffered**, **logging file**, and **logging** Global Configuration mode commands. However, if the **logging** on command is disabled, no messages are sent to these destinations. Only the console receives messages.

Example

The following example enables logging error messages.

```
Console(config)# logging on
```

logging

The **logging** Global Configuration mode command logs messages to a syslog server. Use the **no** form of this command to delete the syslog server with the specified address from the list of syslogs.

Syntax

logging {*ip-address* | *hostname*} [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]

no logging {*ip-address* | *hostname*}

Parameters

- *ip-address* — IP address of the host to be used as a syslog server.
- *hostname* — Specifies the host name of the syslog server. (Range: 1-158 characters)
- *port* — Specifies the port number for syslog messages. (Range: 1-65535)
- *level* — Specifies the severity level of logged messages sent to the syslog servers. Possible values: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational** and **debugging**.
- *facility* — Specifies the facility that is indicated in the message. Possible values: **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local 6**, **ocal7**.
- *text* — Syslog server description. (Range: 1-64 characters)

Default Configuration

The default port number is **514**.

The default logging message level is **informational**.

The default facility is local7.

Command Mode

Global Configuration mode

User Guidelines

Up to 8 syslog servers can be used.

If no specific severity level is specified, the global values apply to each server.

Example

The following example limits logged messages sent to the syslog server with IP address 10.1.1.1 to severity level **critical**.

```
Console(config)# logging 10.1.1.1 severity critical
```

logging console

The **logging console** Global Configuration mode command limits messages logged to the console based on severity. Use the **no** form of this command to disable logging to the console.

Syntax

logging console *level*

no logging console

Parameters

- *level* — Specifies the severity level of logged messages displayed on the console. The possible values are: **emergencies, alerts, critical, errors, warnings, notifications, informational, debugging**.

Default Configuration

The default severity level is **informational**.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example limits logging messages displayed on the console to severity level errors.

```
Console(config)# logging console errors
```

logging buffered

The **logging buffered** Global Configuration mode command limits syslog messages displayed from an internal buffer based on severity. Use the **no** form of this command to cancel using the buffer.

Syntax

logging buffered *level*

no logging buffered

Parameters

- *level* — Specifies the severity level of messages logged in the buffer. The possible values are: **emergencies, alerts, critical, errors, warnings, notifications, informational, debugging**.

Default Configuration

The default severity level is **informational**.

Command Mode

Global Configuration mode

User Guidelines

All the syslog messages are logged to the internal buffer. This command limits the messages displayed to the user.

Example

The following example limits syslog messages displayed from an internal buffer based on severity level **debugging**.

```
Console(config)# logging buffered debugging
```

logging buffered size

The **logging buffered size** Global Configuration mode command changes the number of syslog messages stored in the internal buffer. Use the **no** form of this command to restore the default configuration.

Syntax

logging buffered size *number*

no logging buffered size

Parameters

- *number* — Specifies the maximum number of messages stored in the history table. (Range: 1 - 400)

Default Configuration

The default number of messages is **200**.

Command Mode

Global Configuration mode

User Guidelines

This command takes effect only after Reset.

Example

The following example changes the number of syslog messages stored in the internal buffer to 300.

```
Console(config)# logging buffered size 300
```

clear logging

The **clear logging** Privileged EXEC mode command clears messages from the internal logging buffer.

Syntax

clear logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears messages from the internal logging buffer.

```
Console# clear logging
Clear Logging File [y/n]
```

logging file

The **logging file** Global Configuration mode command limits syslog messages sent to the logging file based on severity. Use the **no** form of this command to cancel using the buffer.

Syntax

logging file *level*

no logging file

Parameters

- *level* — Specifies the severity level of syslog messages sent to the logging file. Possible values are: **emergencies, alerts, critical, errors, warnings, notifications, informational and debugging**.

Default Configuration

The default severity level is **errors.**

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example limits syslog messages sent to the logging file based on severity level **alerts**.

```
Console(config)# logging file alerts
```

clear logging file

The **clear logging file** Privileged EXEC mode command clears messages from the logging file.

Syntax

clear logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example clears messages from the logging file.

```
Console# clear logging file
Clear Logging File [y/n]
```

aaa logging

The **aaa logging** Global Configuration mode command enables logging AAA login events. Use the **no** form of this command to disable logging AAA login events.

Syntax

aaa logging login

no aaa logging login

Parameters

- **login** — Indicates logging messages related to successful login events, unsuccessful login events and other login-related events.

Default Configuration

Logging AAA login events is **enabled**.

Command Mode

Global Configuration mode

User Guidelines

Other types of AAA events are not subject to this command.

Example

The following example enables logging messages related to AAA login events.

```
Console(config)# aaa logging login
```

file-system logging

To control logging file system events, use the file-system logging command in global configuration mode. Use the no form to disable logging.

Syntax

file-system logging copy

no file-system logging copy

file-system logging delete-rename

no file-system logging delete-rename

Parameters

- **copy** — Log messages related to file copy operations.
- **delete-rename** — Log messages related to file deletion and renaming.

Default Configuration

Enabled

Command Mode

Global Configuration

User Guidelines

There are no user guidelines for this command.

Example

```
Console(config)# file-system logging copy
```

management logging

The **management logging** Global Configuration command enables logging management access list (ACL) events. Use the **no** form of this command to disable logging management access list events.

Syntax

management logging deny

no management logging deny

Parameters

- **deny —** Indicates logging messages related to deny actions of management ACLs.

Default Configuration

Logging management ACL events is **enabled**.

Command Mode

Global Configuration mode

User Guidelines

Other types of management ACL events are not subject to this command.

Example

The following example enables logging messages related to deny actions of management ACLs.

```
Console(config)# management logging deny
```

show logging

The **show logging** Privileged EXEC mode command displays the state of logging and the syslog messages stored in the internal buffer.

Syntax

show logging

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the state of logging and the syslog messages stored in the internal buffer.

```
Console# show logging
```

```
Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped (severity).
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.
File logging: level notifications. File Messages: 0 Dropped (severity).
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped (severity).
Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped (severity).
2 messages were not logged (resources)
```

```
Application Filtering Control
Application     Event          Status
-----------     ------         -------
AAA             Login          Enabled
File System     Copy           Enabled
File System     Delete-Rename  Enabled
Management ACL  Deny           Enabled
```

```
Buffer log:
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state
to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state
to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/2, changed state
to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/3, changed state
to up
11-Aug-2004 15:41:43: %SYS-5-CONFIG_I: Configured from memory by console
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/0, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/1, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/2, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet1/3, changed state to down
```

show logging file

The **show logging file** Privileged EXEC mode command displays the state of logging and the syslog messages stored in the logging file.

Syntax

show logging file

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the logging state and the syslog messages stored in the logging file.

```
Console# show logging file

Logging is enabled.
Console logging: level debugging. Console Messages: 0 Dropped (severity).
Buffer logging: level debugging. Buffer Messages: 11 Logged, 200 Max.
File logging: level notifications. File Messages: 0 Dropped (severity).
Syslog server 192.180.2.27 logging: errors. Messages: 6 Dropped (severity).
Syslog server 192.180.2.28 logging: errors. Messages: 6 Dropped (severity).
2 messages were not logged (resources)

Application Filtering Control

Application    Event         Status
-----------    -----         -------
AAA            Login         Enabled
File System    Copy          Enabled
File System    Delete-Rename Enabled
Management ACL Deny          Enabled

Buffer log:

11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface FastEthernet0/
0, changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/0,
changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/1,
changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/2,
changed state to up
11-Aug-2004 15:41:43: %LINK-3-UPDOWN: Interface Ethernet1/3,
changed state to up
11-Aug-2004 15:41:43: %SYS-5-CONFIG_I: Configured from memory by
console
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to up
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet1/0, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet1/1, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet1/2, changed state to down
11-Aug-2004 15:41:39: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Ethernet1/3, changed state to down
```

show syslog-servers

The **show syslog-servers** Privileged EXEC mode command displays the settings of the syslog servers.

Syntax

show syslog-servers

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the settings of the syslog servers.

```
Console# show syslog-servers

Device Configuration

IP address    Port  Severity       Facility  Description
-----------   ----  -------------  --------  -----------
192.180.2.27  514   Informational  local7
192.180.2.27  514   Warning        local7
```

31

System Management Commands

ping

The **ping** User EXEC mode command sends ICMP echo request packets to another node on the network.

Syntax

ping {*ip-address* | *hostname*}[**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]

Parameters

- *ip-address* — IP address to ping.
- *hostname* — Host name to ping. (Range: 1-158 characters)
- *packet_size* — Number of bytes in a packet. The actual packet size is eight bytes larger than the specified size specified because the device adds header information. (Range: 56-1472 bytes)
- *packet_count* — Number of packets to send. If 0 is entered, it pings until stopped. (Range: 0-65535 packets)
- *time_out* — Timeout in milliseconds to wait for each reply. (Range: 50-65535 milliseconds)

Default Configuration

Default packet size is **56** bytes.

Default number of packets to send is.

Default timeout value is **2000** milliseconds.

Command Mode

User EXEC mode

User Guidelines

Press **Esc** to stop pinging.

The following are examples of unsuccessful pinging:

- Destination does not respond. If the host does not respond, a “no answer from host” appears in ten seconds.
- Destination unreachable. The gateway for this destination indicates that the destination is unreachable.
- Network or host unreachable. The device found no corresponding entry in the route table.

Example

The following example displays pinging results:

```
Console> ping 10.1.1.1

Pinging 10.1.1.1 with 64 bytes of data:
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11

Console> ping yahoo.com

Pinging yahoo.com 66.218.71.198 with 64 bytes of data:
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
```

```
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

traceroute

The **traceroute** User EXEC mode command discovers routes that packets actually take when traveling to their destination.

Syntax

traceroute {*destination-ip-address* | *hostname*} [**size** *packet-size*] [**ttl** *max-ttl*] [**count** *packet-count*] [**timeout** *time-out*] [**source** *source-ip-address*] [**tos** *tos*]

Parameters

- *destination-ip-address* — IP address of the destination host.
- *hostname* — Host name of the destination host. (Range: 1-158 characters)
- *packet-size* — Number of bytes in a packet. (Range: 40-1472)
- *max-ttl* — The largest TTL value that can be used. The traceroute command terminates when the destination is reached or when this value is reached. (Range:1-255)
- *packet-count* — The number of probes to be sent at each TTL level. (Range:1-10)
- *time-out* — The number of seconds to wait for a response to a probe packet. (Range:1-60)
- *source-ip-address* — One of the device's interface addresses to use as a source address for the probes. The device normally selects what it feels is the best source address to use.
- *tos* — The Type-Of-Service byte in the IP Header of the packet. (Range: 0-255)

Default Configuration

The default number of bytes in a packet is **40**.

The default maximum TTL value is **0**.

The default number of probes to be sent at each TTL level is **3**.

The default timeout interval in seconds is **3**.

Command Mode

User EXEC mode

User Guidelines

The **traceroute** command takes advantage of the error messages generated by the devices when a datagram exceeds its time-to-live (TTL) value.

The **traceroute** command starts by sending probe datagrams with a TTL value of one. This causes the first device to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A "time exceeded" error message indicates that an intermediate device has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded or when the user interrupts the trace by pressing **Esc**.

Example

The following example discovers the routes that packets will actually take when traveling to their destination.

```
Console> traceroute umaxp1.physics.lsa.umich.edu
```

```
Type Esc to abort.
Tracing the route to umaxp1.physics.lsa.umich.edu
(141.211.101.64)
1 i2-gateway.stanford.edu (192.68.191.83)  0 msec 0 msec 0 msec
2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1
msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162)  1 msec 1 msec
1 msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103)  33 msec 35
msec 35 msec
6 iplsng-kscyng.abilene.ucaid.edu (198.32.8.80)   47 msec 45
msec 45 msec
7 so-0-2-0x1.aa1.mich.net (192.122.183.9)  56 msec  53 msec 54
msec
8 atm1-0x24.michnet8.mich.net (198.108.23.82)  56 msec 56 msec
57 msec
9 * * *
10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu (141.211.5.22) 58 msec 58
msec 58 msec
11 umaxp1.physics.lsa.umich.edu (141.211.101.64)  62 msec 63
msec 63 msec
```

The following table describes significant fields shown above.

Field	Description
1	Indicates the sequence number of the device in the path to the host.
i2-gateway.stanford.edu	Host name of this device.
192.68.191.83	IP address of this device.
1 msec 1 msec 1 msec	Round-trip time for each probe sent.

The following table describes characters that may appear in the **traceroute** command output.

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
F	Fragmentation is required and DF is set.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
R	Fragment reassembly time exceeded.
S	Source route failed.
U	Port unreachable.

telnet

The **telnet** User EXEC mode command enables logging on to a host that supports Telnet.

Syntax

telnet {*ip-address* | *hostname*} [*port*] [*keyword1......*]

Parameters

- *ip-address* — IP address of the destination host.
- *hostname* — Host name of the destination host. (Range: 1-158 characters)

- *port* — A decimal TCP port number, or one of the keywords listed in the Ports table in the User Guidelines.
- *keyword* — One or more keywords listed in the Keywords table in the User Guidelines.

Default Configuration

The default port is the Telnet port (23) on the host.

Command Mode

User EXEC mode

User Guidelines

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To enter a Telnet sequence, press the escape sequence keys (Ctrl-Shift-6) followed by a Telnet command character.

Special Telnet Sequences

Telnet Sequence	Purpose
Ctrl-Shift-6 b	Break
Ctrl-Shift-6 c	Interrupt Process (IP)
Ctrl-Shift-6 h	Erase Character (EC)
Ctrl-Shift-6 o	Abort Output (AO)
Ctrl-Shift-6 t	Are You There? (AYT)
Ctrl-Shift-6 u	Erase Line (EL)

At any time during an active Telnet session, Telnet commands can be listed by pressing the Telnet sequence **Ctrl-Shift-6 ?** at the system prompt.

A sample of this list follows. Note that the Ctrl-Shift-6 sequence appears as ^^ on the screen.

```
Console> ‘Ctrl-shift-6’ ?
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
Ctrl-shift-6 x suspends the session (return to system command
prompt)
```

Several concurrent Telnet sessions can be opened and switched. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence keys (Ctrl-Shift-6) and x to return to the system command prompt. Then open a new connection with the **telnet** User EXEC mode command.

Keywords Table

Options	Description
/echo	Enables local echo.
/quiet	Prevents onscreen display of all messages from the software.
/source-interface	Specifies the source interface.
/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
Ctrl-Shift-6 x	Return to System Command Prompt

Ports Table

Keyword	Description	Port Number
BGP	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111

Keyword	Description	Port Number
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

This command lists concurrent telnet connections to remote hosts that were opened by the current telnet session to the local device. It does not list telnet connections to remote hosts that were opened by other telnet sessions.

Example

The following example displays connecting to 176.213.10.50 via Telnet.

```
Console> telnet 176.213.10.50
Esc U sends telnet EL
```

resume

The **resume** User EXEC mode command enables switching to another open Telnet session.

Syntax

resume [*connection*]

Parameters

- *connection* — The connection number. (Range: 1-4 connections)

Default Configuration

The default connection number is that of the most recent connection.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following command switches to open Telnet session number 1.

```
Console> resume 1
```

reload

The **reload** Privileged EXEC mode command reloads the operating system.

Syntax

reload

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Caution should be exercised when resetting the device, to ensure that no other activity is being performed. In particular, the user should verify that no configuration files are being downloaded at the time of reset.

Example

The following example reloads the operating system.

```
Console# reload
This command will reset the whole system and disconnect your
current session. Do you want to continue (y/n) [n]?
```

hostname

The **hostname** Global Configuration mode command specifies or modifies the device host name. Use the **no** form of the command to remove the existing host name (i.e., restore the default hostname "**Console**").

Syntax

hostname *name*

no hostname

Parameters

- *name* — The host name of the device. (Range: 1-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the device host name.

```
Console(config)# hostname enterprise
enterprise(config)#
```

service cpu-utilization

The **service cpu-utilization** Global Configuration mode command enables measuring CPU utilization. Use the no form of the command to restore the default configuration.

Syntax

service cpu-utilization

no service cpu-utilization

Default Configuration

Enabled.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

This example enables measuring CPU utilization.

```
Console(config)# service cpu-utilization
```

show cpu utilization

The **show cpu utilization** Privileged EXEC mode command displays information about CPU utilization.

Syntax

show cpu utilization

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **service cpu-utilization** Global Configuration command to enable measuring CPU utilization.

Example

This example shows how to display CPU utilization information.

```
Console# show cpu-utilization
CPU utilization service is on.
CPU utilization
--------------------------
five seconds: 5%; one minute: 3%; five minutes: 3%
```

show users

The **show users** Privileged EXEC mode command displays information about the active users.

Syntax

show users

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information about the active users.

```
Console# show users

Username   Protocol      Location
--------   ----------    -----------
Bob        Serial
John       SSH           172.16.0.1
Robert     HTTP          172.16.0.8
Betty      Telnet        172.16.1.7
```

show sessions

The **show sessions** Privileged EXEC mode command lists open Telnet sessions.

Syntax

show sessions

Default Configuration

There is no default configuration for this command.

Command Mode

Privileged EXEC mode

User Guidelines

The command shows the telnet sessions to remote hosts opened by the present telnet session to the local device. This command will not show telnet sessions to remote hosts opened by other telnet sessions to the local device.

Example

The following example lists open Telnet sessions.

```
Console# show sessions

Connection  Host           Address        Port    Byte
----------  -------------  ---------      ----    ----
1           Remote device  172.16.1.1     23      89
2           172.16.1.2     172.16.1.2     23      8
```

The following table describes significant fields shown above.

Field	Description
Connection	Connection number
Host	Remote host to which the device is connected through a Telnet session.
Address	IP address of the remote host.
Port	Telnet TCP port number
Byte	Number of unread bytes for the user to see on the connection.

show system

The **show system** Privileged EXEC mode command displays system information.

Syntax

show system [unit *unit***]**

Parameters

- *unit* — Specifies the number of the unit. (Range: 1-8)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the system information.

```
Console# show system

System Description:           Corporate
System Up Time (days,hour:min:sec):1,22:38:21
System Contact:
System Name:                  RS1
System location:
System MAC Address:           0010.B5F4.0001
Temperature Sensors:

Unit       Sensor          Temperature   Status
                           (Celsius)
--------   ----------      ----------    --------
1          1               41            OK
1          2               41            OK
2          1               42            OK
           2               42            OK

Unit       Power supply    Source        Status
--------   ------------    ---------     --------
1          Main            AC            OK
2          Secondary       AC            OK

Unit       FAN             Status
--------   ----------      ---------     --------
1          Backplane       OK
2          CPU             OK
```

show version

The **show version** Privileged EXEC mode command displays system version information.

Syntax

show version [**unit** *unit*]

Parameters

- *unit*— Specifies the number of the unit.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays system version information (only for demonstration purposes).

```
console# show version

SW version    1.0.2 ( date  14-Jul-2008 time  10:19:35 )
Boot version    1.0.2 ( date  13-Nov-2007 time  14:11:51 )
HW version    00.00.01
```

show system tcam utilization

The **show system tcam** Privileged EXEC mode command displays the Ternary Content Addressable Memory (TCAM) utilization.

Syntax

show system tcam utilization [unit *unit***]**

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays information on features control.

```
Console> show system tcam utilization
TCAM utilization: 58%
```

32

TACACS+ Commands

tacacs-server host

The **tacacs-server host** Global Configuration mode command specifies a TACACS+ host. Use the **no** form of the command to delete the specified name or address.

Syntax

tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *key-string*] [**source** *source*] [**priority** priority]

no tacacs-server host {*ip-address* | *hostname*}

Parameters

- *ip-address* — IP address of the TACACS+ server.
- *hostname* — Host name of the TACACS+ server. (Range: 1-158 characters)
- **single-connection** — Indicates a single-connection. Rather than have the device open and close a TCP connection to the daemon each time it must communicate, the single-connection option maintains a single open connection between the device and the daemon.
- *port-number* — Specifies a server port number. The host is not used for authentication if the port number is set to 0. (Range: 0-65535)
- *timeout* — Specifies the timeout value in seconds. (Range: 1-30)
- *key-string* — Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter “”. (Range: 0-128 characters)

- *source* — Specifies the source IP address to use for the communication. 0.0.0.0 indicates a request to use the IP address of the outgoing IP interface.
- *priority* — Determines the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0-65535)

Default Configuration

No TACACS+ host is specified.

If no port number is specified, default port number **49** is used.

If no host-specific timeout, key-string or source value is specified, the global value is used.

If no TACACS+ server priority is specified, default priority **0** is used.

Command Mode

Global Configuration mode

User Guidelines

Multiple **tacacs-server host** commands can be used to specify multiple hosts.

Example

The following example specifies a TACACS+ host.

```
Console(config)# tacacs-server host 172.16.1.1
```

tacacs-server key

The **tacacs-server key** Global Configuration mode command sets the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. Use the **no** form of the command.

Syntax

tacacs-server key *key-string*

no tacacs-server key

Parameters

- *key-string* — Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. (Range: 0-128 characters)

Default Configuration

Empty string.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the authentication encryption key for all TACACS+ servers.

```
Console(config)# tacacs-server key enterprise
```

tacacs-server timeout

The **tacacs-server timeout** Global Configuration mode command sets the interval during which the device waits for a TACACS+ server to reply. Use the **no** form of the command to restore the default configuration.

Syntax

tacacs-server timeout *timeout*

no tacacs-server timeout

Parameters

- *timeout* — Specifies the timeout value in seconds. (Range: 1-30)

Default Configuration

5 seconds

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the timeout value to 30 for all TACACS+ servers.

```
Console(config)# tacacs-server timeout 30
```

tacacs-server source-ip

The **tacacs-server source-ip** Global Configuration mode command configures the source IP address to be used for communication with TACACS+ servers. Use the **no** form of the command to restore the default configuration.

Syntax

tacacs-server source-ip *source*

no tacacs-server source-ip *source*

Parameters

- *source* — Specifies the source IP address.

Default Configuration

The source IP address is the address of the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example specifies the source IP address for all TACACS+ servers.

```
Console(config)# tacacs-server source-ip 172.16.8.1
```

show tacacs

The **show tacacs** Privileged EXEC mode command displays configuration and statistical information about a TACACS+ server.

Syntax

show tacacs [*ip-address*]

Parameters

- *ip-address* — Name or IP address of the TACACS+ server.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays configuration and statistical information about a TACACS+ server.

```
Console# show tacacs

Device Configuration
--------------------

IP address Status    Port Single Connection TimeOut Source IPPriority
---------- --------- ---- ----------------- ------- -----------------
172.16.1.1 Connected 48   No                Global  Global   1
```

```
Global values
-------------
TimeOut: 3
```

33

User Interface Commands

login

The **login** User EXEC mode command changes a login username.

Syntax

login

Default Configuration

This command has no default configuration.

Command Mode

User EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters Privileged EXEC mode and logs in with username admin.

```
Console> login
User Name:admin
Password:*****
Console#
```

configure

The **configure** Privileged EXEC mode command enters the Global Configuration mode.

Syntax

configure

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters Global Configuration mode.

```
Console# configure
Console(config)#
```

exit (configuration)

The **exit** command exits from any configuration mode to the next highest mode in the CLI mode hierarchy.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

All configuration modes

User Guidelines

There are no user guidelines for this command.

Example

The following example changes the configuration mode from Interface Configuration mode to Privileged EXEC mode.

```
Console(config-if)# exit
Console(config)# exit
Console#
```

exit(EXEC)

The **exit** Privileged/User EXEC mode command closes an active terminal session by logging off the device.

Syntax

exit

Default Configuration

This command has no default configuration.

Command Mode

Privileged and User EXEC modes

User Guidelines

There are no user guidelines for this command.

Example

The following example closes an active terminal session.

```
Console> exit
```

end

The **end** command ends the current configuration session and returns to the Privileged EXEC mode.

Syntax

end

Default Configuration

This command has no default configuration.

Command Mode

All configuration modes.

User Guidelines

There are no user guidelines for this command.

Example

The following example changes from Global Configuration mode to Privileged EXEC mode.

```
Console(config)# end
Console#
```

help

The **help** command displays a brief description of the help system.

Syntax

help

Default Configuration

This command has no default configuration.

Command Mode

All command modes

User Guidelines

There are no user guidelines for this command.

Example

The following example describes the help system.

```
Console# help
```

```
Help may be requested at any point in a command by entering a
question mark ‘?’. If nothing matches the currently entered
incomplete command, the help list is empty. This indicates that
for a query at this point, there is no command matching the
current input. If the request is within a command, enter
backspace and erase the entered characters to a point where the
request results in a display.
```

```
Help is provided when:
```

1. There is a valid command and a help request is made for entering a parameter or argument (e.g. ‘show ?’). All possible parameters or arguments for the entered command are displayed.

2. An abbreviated argument is entered and a help request is made for arguments matching the input (e.g. ‘show pr?’).

history

The **history** Line Configuration mode command enables the command history function. Use the **no** form of the command to disable the command history function.

Syntax

history

no history

Default Configuration

The command history function is enabled.

Command Mode

Line Configuration mode

User Guidelines

This command enables the command history function for a specified line. Use the **terminal history** user EXEC mode command to enable or disable the command history function for the current terminal session.

Example

The following example enables the command history function for Telnet.

```
Console(config)# line telnet
Console(config-line)# history
```

history size

The **history size** Line Configuration mode command configures the command history buffer size for a particular line. Use the **no** form of this command to reset the command history buffer size to the default configuration.

Syntax

history size *number-of-commands*

no history size

Parameters

- *number-of-commands*—Number of commands that the system records in its history buffer. (Range: 10 - 206)

Default Configuration

The default history buffer size is **10**.

Command Mode

Line Configuration mode

User Guidelines

This command configures the command history buffer size for a particular line. To configure the command history buffer size for the current terminal session, use the **terminal history size** User EXEC mode command.

Example

The following example changes the command history buffer size to 100 entries for a particular line.

```
Console(config)# line telnet
Console(config-line)# history size 100
```

terminal history

The **terminal history** User EXEC mode command enables the command history function for the current terminal session. Use the **no** form of this command to disable the command history function.

Syntax

terminal history

no terminal history

Default Configuration

The default configuration for all terminal sessions is defined by the **history** line configuration command.

Command Mode

User EXEC mode

User Guidelines

The command enables the command history for the current session. The default is determined by the history line configuration command.

Example

The following example disables the command history function for the current terminal session.

```
Console> terminal no history
```

terminal history size

The **terminal history size** User EXEC mode command configures the command history buffer size for the current terminal session. Use the **no** form of this command to reset the command history buffer size to the default setting.

Syntax

terminal history size *number-of-commands*

terminal no history size

Parameters

- *number-of-commands* — Specifies the number of commands the system may record in its command history buffer. (Range: 10-206)

Default Configuration

The default command history buffer size is 10.

Command Mode

User EXEC mode

User Guidelines

The **terminal history size** user EXEC command configures the size of the command history buffer for the current terminal session. To change the default size of the command history buffer, use the **history** line configuration command.

The maximum number of commands in all buffers is 256.

Example

The following example configures the command history buffer size to 20 commands for the current terminal session.

```
Console> terminal history size 20
```

terminal datadump

The **terminal datadump** User EXEC mode command enables dumping all the output of a show command without prompting. Use the **no** form of this command to disable dumping.

Syntax

terminal datadump

terminal no datadump

Default Configuration

Data dump is disabled.

Command Mode

User EXEC mode

User Guidelines

By default, a **More** prompt is displayed when the output contains more lines than can be displayed on the screen. Pressing the **Enter** key displays the next line; pressing the Spacebar displays the next screen of output. The datadump command enables dumping all output immediately after entering the show command.

This command is relevant only for the current session.

Example

This example dumps all output immediately after entering a show command.

```
Console> terminal datadump
```

debug-mode

The **debug-mode** Privileged EXEC mode command switches to debug mode.

Syntax

debug-mode

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables the debug command interface.

```
console(config)#
console# debug
>debug
Enter DEBUG Password: *****
DEBUG>
```

show history

The **show history** Privileged EXEC mode command lists the commands entered in the current session.

Syntax

show history

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

The buffer includes executed and unexecuted commands.

Commands are listed from the first to the most recent command.

The buffer remains unchanged when entering into and returning from configuration modes.

Example

The following example displays all the commands entered while in the current Privileged EXEC mode.

```
Console# show version

SW version 3.131 (date 23-Jul-2005 time 17:34:19)
HW version 1.0.0


Console# show clock

15:29:03 Jun 17 2005
```

```
Console# show history

show version
show clock
show history
3 commands were logged (buffer size is 10)
```

do

The **do** command in any configuration mode executes an EXEC-level command from Global Configuration mode or any Configuration submode.

Syntax

do *command*

Parameters

- *command* — The EXEC command to be executed.

Default Configuration

This command has no default configuration.

Command Mode

All Configuration modes

User Guidelines

There are no user guidelines for this command.

Example

The following example shows to display current privilege level.

```
Console (Config)# do show vlan

VLAN    Name        Ports      Type      Authorization
------- ----------  ---------- --------- -------------
1       default     e1-e2      Other     Required
                    e9-e12
10      VLAN0010    e3-e4      dynamic   Required
11      VLAN0011    e1-e2      static    Required
20      VLAN0020    e3-e4      static    Required
21      VLAN021                static    Required
30      VLAN0030               static    Required
31      VLAN0031               static    Required
91      VLAN0011    e1-e2      static    Not Required
3978    Guest VLAN  e17        static    Guest
```

34

VLAN Commands

switchport protected

The **switchport protected** Interface Configuration mode command overrides the FDB decision, and sends all Unicast, Multicast and Broadcast traffic to an uplink port. Use the **no** form of this command to disable overriding the FDB decision.

Syntax

switchport protected {**ethernet** port | **port-channel** port-channel-number}

no switchport protected

Parameters

- *port* — Specifies the uplink Ethernet port.
- *port-channel-number* — Specifies the uplink port-channel.

Default Configuration

Switchport protected is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- Private VLAN Edge (PVE) only operates on interfaces that do not have an IP address.

- PVE only operates on interfaces that do not belong to VLANs that have IP addresses.
- PVE supports private communication by isolating PVE-defined ports and ensuring that all Unicast, Broadcast and Multicast traffic from these ports is only forwarded to uplink port(s).
- PVE requires only one VLAN on each device, but not on every port; this reduces the number of VLANs required by the device. Private VLANs and the default VLAN function simultaneously in the same device.

Example

This example configures ethernet port 2 as a protected port, so that all traffic is sent to its uplink (Ethernet port 3).

```
Console(config)# interface ethernet 2
Console(config-if)# switchport protected ethernet 3
```

switchport protected-port

Use the **switchport protected-port** interface configuration command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. Use the **no** form of this command to disable protection on the port.

NOTE The SPS208G and SPS224G4 do not support this command.

Syntax

switchport protected-port

no switchport protected-port

Parameters

This command has no arguments or keywords.

Default Configuration

Unprotected

Command Mode

Interface configuration (Ethernet, port-channel)

User Guidelines

Use this command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch.

NOTE The packet is still subject to the FDB decision and to all filtering rules.

switchport protected-port fastethernet

Use the **switchport protected-port fastethernet** global configuration command set the FE ports as protected ports. Use the **no** form of this command to set the FE ports as unprotected ports.

NOTE This command is supported in SPS2xx devices.

Syntax

switchport protected-port fastethernet

no switchport protected-port fastethernet

Parameters

This command has no arguments or keywords.

Default Configuration

Unprotected

Command Mode

Global configuration

Usage Guidelines

This command configures all the FE ports as protected ports.

vlan database

The **vlan database** Global Configuration mode command enters the VLAN Configuration mode.

Syntax

vlan database

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enters the VLAN database mode.

```
Console(config)# vlan database
Console(config-vlan)#
```

vlan

The **vlan** VLAN Database mode command creates a VLAN. Use the **no** form of this command to delete a VLAN.

Syntax

vlan *vlan-range*

no vlan *vlan-range*

Parameters

- *vlan-range* — Specifies a list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs. (Range: 2-4094)

Default Configuration

This command has no default configuration.

Command Mode

VLAN Database mode

User Guidelines

There are no user guidelines for this command.

Example

The following example creates the VLAN number 1972.

```
Console(config)# vlan database
Console(config-vlan)# vlan 1972
```

default-vlan vlan

The **default-vlan vlan** VLAN Configuration mode command defines the default VLAN. Use the **no** form of this command to return to default.

Syntax

default-vlan vlan *vlan-id*

no default-vlan vlan

Parameters

- *vlan-id* — VLAN ID of the default VLAN.

Default Configuration

The default configuration is disabled.

Command Mode

VLAN Configuration

User Guidelines

No user guidelines for this command.

Example

The following example defines the default VLAN.

```
Console(config-vlan)# default-vlan vlan
```

interface vlan

The **interface vlan** Global Configuration mode command enters the Interface Configuration (VLAN) mode.

Syntax

interface vlan *vlan-id*

Parameters

- *vlan-id* — Specifies an existing VLAN ID.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

In case the VLAN doesn't exist ('ghost VLAN') only partial list of the commands are available under the interface VLAN context.

The commands that are supported for VLAN that do not exist are:

1. IGMP snooping control
2. Bridge Multicast configuration

Example

The following example configures VLAN 1 with IP address 131.108.1.27.

```
Console(config)# interface vlan 1
Console(config-if)# ip address 131.108.1.27
```

interface range vlan

The **interface range vlan** Global Configuration mode command enables simultaneously configuring multiple VLANs.

Syntax

interface range vlan {*vlan-range* | **all**}

Parameters

- *vlan-range* — Specifies a list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces; a hyphen designates a range of IDs. (Range: 2-4094)
- **all** — All existing static VLANs.

Default Configuration

This command has no default configuration.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and execution of the command continues on the other interfaces.

Configuring all ports may consume an excessive amount of time. Define only the required ports to save time.

Example

The following example groups VLANs 221 through 228 and 889 to receive the same command.

```
Console(config)# interface range vlan 221-228,889
Console(config-if)#
```

name

The **name** Interface Configuration mode command adds a name to a VLAN. Use the **no** form of this command to remove the VLAN name.

Syntax

name *string*

no name

Parameters

- *string* — Unique name to be associated with this VLAN. (Range: 1-32 characters)

Default Configuration

No name is defined.

Command Mode

Interface Configuration (VLAN) mode. Cannot be configured for a range of interfaces (range context).

User Guidelines

The name string may include numbers and other characters (#,@,% etc.) but no spaces.

Example

The following example gives VLAN number 19 the name **Marketing**.

```
Console(config)# interface vlan 19
Console(config-if)# name Marketing
```

switchport mode

The **switchport mode** Interface Configuration mode command configures the VLAN membership mode of a port. Use the **no** form of this command to restore the default configuration.

Syntax

switchport mode {**access** | **trunk** | **general** | **customer**}

no switchport mode

Parameters

- **access** — Indicates an untagged layer 2 VLAN port.
- **trunk** — Indicates a trunking layer 2 VLAN port.
- **general** — Indicates a full 802-1q supported VLAN port.
- **customer** — The port is connected to customer equipment. Used when the switch is in a provider network.

Default Configuration

All ports are in access mode, and belong to the default VLAN (whose VID=1).

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines.

Example

The following example configures Ethernet port 1 as an untagged layer 2 VLAN port.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode access
```

switchport protected

The **switchport protected** Interface Configuration mode command overrides the FDB decision, and sends all Unicast, Multicast and Broadcast traffic to an uplink port. Use the **no** form of this command to disable overriding the FDB decision.

Syntax

switchport protected {**ethernet** port | **port-channel** port-channel-number}

no switchport protected

Parameters

- *port* — Uplink Ethernet port.
- *port-channel-number* — Uplink port-channel.

Default Configuration

Switchport protected is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- Private VLAN Edge (PVE) only operates on interfaces that do not have an IP address.
- PVE only operates on interfaces that do not belong to VLANs that have IP addresses.
- PVE supports private communication by isolating PVE-defined ports and ensuring that all Unicast, Broadcast and Multicast traffic from these ports is only forwarded to uplink ports.
- PVE requires only one VLAN on each device, but not on every port; this reduces the number of VLANs required by the device. Private VLANs and the default VLAN function simultaneously in the same device.

Example

This example configures ethernet port 2 as a protected port, so that all traffic is sent to its uplink (Ethernet port 3).

```
Console(config)# interface ethernet 2
Console(config-if)# switchport protected ethernet 3
```

switchport access vlan

The **switchport access vlan** Interface Configuration mode command configures the VLAN ID when the interface is in access mode. Use the **no** form of this command to restore the default configuration.

Syntax

switchport access vlan {*vlan-id*}

no switchport access vlan

Parameters

- *vlan-id* — Specifies the ID of the VLAN to which the port is configured.

Default Configuration

All ports belong to VLAN 1.

Command Mode

Interface configuration (Ethernet, port-channel) mode

User Guidelines

The command automatically removes the port from the previous VLAN and adds it to the new VLAN.

Example

The following example configures a VLAN ID of 23 to the untagged layer 2 VLAN Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport access vlan 23
```

switchport access multicast-tv vlan

The **switchport access multicast-tv vlan** Interface Configuration mode command enables receiving Multicast transmissions from a VLAN that is not the Access port VLAN, while maintaining the L2 segregation with subscribers on different Access port VLANs. Use the **no** form of this command to disable receiving Multicast transmissions.

Syntax

switchport access multicast-tv vlan *vlan-id*

no switchport access multicast-tv vlan

Parameters

- *vlan-id* — Specifies the ID of the VLAN to which the port is configured.

Default Configuration

The configuration is disabled.

Command Mode

Interface configuration (Ethernet, port-channel) mode

User Guidelines

The user cannot transmit Multicast transmissions on the Multicast TV VLAN.

Example

The following example adds VLANs 2,5-6 to the allowed list.

```
console(config-if)# switchport trunk allowed vlan add 2,5-6
```

switchport trunk allowed vlan

The **switchport trunk allowed vlan** Interface Configuration (Ethernet, port-channel) mode command adds or removes VLANs to or from a trunk port.

Syntax

switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list*}

Parameters

- **add** *vlan-list* — List of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

- **remove** *vlan-list* — List of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

This command has no default configuration.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example adds VLANs 1, 2, 5 to 6 to the allowed list.

```
console(config-if)# switchport trunk allowed vlan add 1-2,5-6
```

switchport trunk native vlan

The **switchport trunk native vlan** Interface Configuration mode command defines the native VLAN when the interface is in trunk mode. Use the **no** form of this command to restore the default configuration.

Syntax

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

Parameters

- *vlan-id*— Specifies the ID of the native VLAN.

Default Configuration

VID=1.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command adds the port as a member in native VLAN. If the port is already in the VLAN (as allowed) it will automatically change the last entry to native.

The command adds the port as a member in native VLAN 2. If the port is already configured as a native VLAN 3 it will automatically change the last entry (VLAN 2). Only one native VLAN can be configured to the port.

Example

The following example configures VLAN number 123 as the native VLAN when Ethernet port 1 is in trunk mode.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode trunk
Console(config-if)# switchport trunk native vlan 123
```

switchport general allowed vlan

The **switchport general allowed vlan** Interface Configuration mode command adds or removes VLANs from a general port.

Syntax

switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]

switchport general allowed vlan remove *vlan-list*

Parameters

- **add** *vlan-list* — Specifies the list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list* — Specifies the list of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **tagged** — Indicates that the port transmits tagged packets for the VLANs.
- **untagged** — Indicates that the port transmits untagged packets for the VLANs.

Default Configuration

If the port is added to a VLAN without specifying tagged or untagged, the default setting is tagged.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command enables changing the egress rule (for example from tagged to untagged) without first removing the VLAN from the list.

Example

The following example adds VLANs 2, 5, and 6 to the allowed list of Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode general
Console(config-if)# switchport general allowed vlan add 2,5-6
tagged
```

switchport general pvid

The **switchport general pvid** Interface Configuration mode command configures the PVID when the interface is in general mode. Use the **no** form of this command to restore the default configuration.

Syntax

switchport general pvid *vlan-id*

no switchport general pvid

Parameters

- *vlan-id* — Specifies the PVID (Port VLAN ID).

Default Configuration

If the default VLAN is enabled, PVID = 1. Otherwise, PVID=4095.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures the PVID for Ethernet port 1, when the interface is in general mode.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode general
Console(config-if)# switchport general pvid 234
```

switchport general ingress-filtering disable

The **switchport general ingress-filtering disable** Interface Configuration mode command disables port ingress filtering. Use the **no** form of this command to restore the default configuration.

Syntax

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Default Configuration

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example disables port ingress filtering on Ethernet port 1

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode general
Console(config-if)# switchport general ingress-filtering
disable
```

switchport general acceptable-frame-type tagged-only

The **switchport general acceptable-frame-type tagged-only** Interface Configuration mode command discards untagged frames at ingress. Use the **no** form of this command to restore the default configuration.

Syntax

switchport general acceptable-frame-type tagged-only

no switchport general acceptable-frame-type tagged-only

Default Configuration

All frame types are accepted at ingress.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures Ethernet port 1 to discard untagged frames at ingress.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode general
Console(config-if)# switchport general acceptable-frame-type
tagged-only
```

switchport customer vlan

The **switchport customer vlan** Interface Configuration (Ethernet, port-channel) mode command sets the port's VLAN when the interface is in customer mode. Use the **no** form of this command to restore the default configuration.

Syntax

switchport customer vlan *vlan-id*

no switchport customer vlan

Parameters

- *vlan-id* — VLAN ID of the customer.

Default Configuration

No VLAN is configured.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example configures Ethernet port 1 to discard untagged frames at ingress.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport customer vlan
```

switchport customer multicast-tv vlan

The **switchport customer multicast-tv vlan** interface configuration command enables the receiving of Multicast transmissions from a VLAN that is not the Customer port's VLAN, while keeping the L2 segregation with subscribers on different Customer port VLANs.

Syntax

switchport customer multicast-tv vlan {**add** *vlan-list* | **remove** *vlan-list*}

Parameters

- *vlan-list* — List of Multicast TV VLANs.

Default Configuration

The port is not member in any Multicast TV VLAN.

Command Mode

Interface configuration (Ethernet, port-channel).

Command Usage

The user cannot transmit Multicast transmissions on Multicast TV VLANs.

Example

The following example configures port e1 to enable receiving Multicast transmissions from a VLAN that is not the customer port's VLAN.

```
Console (config-if)# switchport customer multicast-tv vlan add
3000
```

switchport forbidden vlan

The **switchport forbidden vlan** Interface Configuration mode command forbids adding specific VLANs to a port. Use the **remove** parameter for this command to restore the default configuration.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}

Parameters

- **add** *vlan-list* — Specifies the list of VLAN IDs to be added. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.
- **remove** *vlan-list* — Specifies the list of VLAN IDs to be removed. Separate nonconsecutive VLAN IDs with a comma and no spaces. A hyphen designates a range of IDs.

Default Configuration

All VLANs are allowed.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

This command can be used to prevent GVRP from automatically making the specified VLANs active on the selected ports.

Example

The following example forbids adding VLAN IDs 234 to 256 to Ethernet port 1.

```
Console(config)# interface ethernet 1
Console(config-if)# switchport mode trunk
Console(config-if)# switchport forbidden vlan add 234-256
```

show interfaces protected-ports

Use the **show interfaces protected-ports** EXEC command to show protected ports configuration.

NOTE This command is supported in SPS20xx devices.

Syntax

show interfaces protected-ports

Default Configuration

Defaults

Command Mode

EXEC

Example

```
Console> show interfaces protected

Interface    State
----------  ----------------
1/1         Unprotected
```

```
1/2          Protected
1/3          Protected
1/4          Protected
```

show protected-ports fastethernet

Use the **show protected-ports fastethernet** EXEC command to show protected ports configuration.

NOTE This command is supported in SPS2xx devices.

Syntax

show protected-ports fastethernet

Default Configuration

Defaults

Command Mode

EXEC

Example

```
Console> show protected-ports fastethernet

GE protected-ports state:  Unprotected
FE protected-ports state:  Protected
```

show vlan

The **show vlan** Privileged EXEC mode command displays VLAN information.

Syntax

show vlan [tag *vlan-id* | **name** *vlan-name*]

Parameters

- *vlan-id* — specifies a VLAN ID
- *vlan-name* — Specifies a VLAN name string. (Range: 1-32 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays all VLAN information.

```
Console# show vlan

VLAN  Name        Ports  Type      Authorization
----  --------    -----  ----      -------------
1     default     1,2    other     Required
10    VLAN0010    1      dynamic   Required
11    VLAN0011    1      static    Required
20    VLAN0020    1      static    Required
21    VLAN0021           static    Required
```

```
30    VLAN0030          static    Required
31    VLAN0031          static    Required
91    VLAN0011    1     static    Not Required
3978  Guest VLAN  1     guest     --
```

show vlan multicast-tv

The **show vlan multicast-tv** Privileged EXEC mode command displays information on the source ports and receiver ports of Multicast-TV VLAN.

Syntax

show vlan multicast-tv vlan *vlan-id*

Parameters

- *vlan-id* — VLAN ID value.

Default Configuration

The default configuration is disabled.

Command Mode

Privileged EXEC mode

User Guidelines

No user guidelines for this command.

Example

The following example displays information on the source ports and receiver ports of Multicast-TV VLAN.

```
Console # show vlan multicast-tv vlan 1000
```

```
Source ports    Receiver Ports
-------------   ----------------------
e8, e9          e1-e4, e12-e18, e22-e24
```

show interfaces switchport

The **show interfaces switchport** Privileged EXEC mode command displays the switchport configuration.

Syntax

show interfaces switchport {**ethernet** *interface* | **port-channel** *port-channel-number*}

Parameters

- *interface* — A valid Ethernet port number.
- *port-channel-number* — A valid port-channel number.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the switchport configuration for Ethernet port 10 map protocol protocols-group.

```
Console# show interface switchport ethernet 10

Port: 10
Port mode: General
GVRP Status: General
Ingress Filtering: True
Acceptable Frame Type: AdmitAll
Ingress UnTagged VLAN (NATIVE): 6
Protected: Enabled, Uplink is 2


Port is member in:

Vlan    Name    Egress rule   Port Membership Type
----    ------  -----------   --------
2       2       Untagged      Static
3       3       Tagged        Static
6       6       Tagged        Static


Forbidden VLANS:
VLAN    Name
----    ----
5       5


Classification rules:

Protocol-based VLANs:


Group ID   Vlan ID
----       -----------
213        3
```

35

Web Server Commands

ip http server

The **ip http server** Global Configuration mode command enables configuring the device from a browser. Use the no form of this command to disable this function.

Syntax

ip http server

no ip http server

Default Configuration

HTTP server is enabled.

Command Mode

Global Configuration mode

User Guidelines

Only a user with access level 15 can use the Web server.

Example

The following example enables configuring the device from a browser.

```
Console(config)# ip http server
```

ip http port

To specify the TCP port to be used by the web browser interface, use the ip http port global configuration command. To use the default port, use the no form of this command.

Syntax

ip http port *port-number*

no ip http port

Parameters

- *port-number* — Port number for use by the HTTP server. Range: 0 - 65534

Default Configuration

80

Command Mode

Global configuration

Usage Guidelines

Specifying 0 as the port number effectively disables HTTP access to the device.

Examples

```
Console(config)# ip http port 100
```

ip http exec-timeout

The **ip http exec**-timeout Global Configuration mode command sets the interval that the system waits for user input in http sessions, prior to automatic logoff. Use the **no** form of this command to return to default.

Syntax

ip http exec-timeout *minutes* [*seconds*]

no ip http exec-timeout

Parameters

- *minutes* — Integer that specifies the number of minutes. Range: 1 - 65535.
- *seconds* — Additional time intervals in seconds. Range: 0 - 59.

Default Configuration

The default is **10min**.

Command Mode

Global Configuration mode

User Guidelines

This command also configures the exec-timeout for HTTPS in case the HTTPS timeout was not set.

To specify no timeout, enter the ip https exec-timeout 0 0 command.

Example

The following example sets the interval that the system waits to user input in http sessions before automatic logoff.

```
Console(config)# ip http exec-timeout 10 [30]
```

ip https server

The **ip https server** Global Configuration mode command enables configuring the device from a secured browser. Use the **no** form of this command to restore the default configuration.

Syntax

ip https server

no ip https server

Default Configuration

Disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **crypto certificate generate** Global Configuration mode command to generate an HTTPS certificate.

Example

The following example enables configuring the device from a secured browser.

```
Console(config)# ip https server
```

ip https port

The **ip https port** Global Configuration mode command specifies the TCP port used by the server to configure the device through the Web browser. Use the **no** form of this command to restore the default configuration.

Syntax

ip https port *port-number*

no ip https port

Parameters

- *port-number* — Port number to be used by the HTTP server. Range: 0-65535.

Default Configuration

The default port number is 443.

Command Mode

Global Configuration mode.

User Guidelines

Specifying 0 as the port number effectively disables HTTP access to the device.

Example

The following example configures the https port number to 100.

```
Console(config)# ip https port 100
```

ip https exec-timeout

The **ip https exec-timeout** Global Configuration mode command sets the interval that the system waits for user input in https sessions, prior to automatic logoff. Use the **no** form of this command to return to default.

Syntax

ip https exec-timeout *minutes* [*seconds*]

no ip https exec-timeout

Parameters

- *minutes* — Integer that specifies the number of minutes. Range: 1 - 65535.
- *seconds* — Additional time intervals in seconds. Range: 0 - 59.

Default Configuration

The exec-timeout set by the **ip http exec-timeout** command.

Command Mode

Global Configuration mode.

User Guidelines

To specify no timeout, enter the **ip https exec-timeout 0 0** command.

Example

The following example set the interval that the system waits to user input in https sessions before automatic logoff.

```
Console(config)# ip https exec-timeout
```

ip https certificate

To configure the active certificate for HTTPS, use the ip https certificate global configuration command. Use the no form of this command to return to default.

Syntax

ip https certificate *number*

no ip https certificate

Parameters

- *number* — Specifies the certificate number. Range: 1 digit, product specific

Default Configuration

Certificate number 1.

Command Mode

Global configuration

Usage Guidelines

You should use the **crypto certificate generate** command in order to generate an HTTPS certificate.

Examples

```
Console(config)# ip https certificate 1
```

show ip http

The **show ip http** Privileged EXEC mode command displays the HTTP server configuration.

Syntax

show ip http

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the HTTP server configuration.

```
Console# show ip http

HTTP server enabled. Port: 80
Interactive timeout: 10 minutes
```

show ip https

The **show ip https** Privileged EXEC mode command displays the HTTPS server configuration.

Syntax

show ip https

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the HTTP server configuration.

```
Console# show ip https
```

```
HTTPS server enabled. Port: 443
Certificate 1 is not active.
 Issued by : C=  , ST= , L= , CN=10.6.41.138, O= , OU=
 Valid From: Apr 30 20:51:54 2003 GMT
 Valid to: Apr 29 20:51:54 2004 GMT
 Subject: C=  , ST= , L= , CN=10.6.41.138, O= , OU=
 SHA1 Fingerprint: B3536E86 9487B229 C0A44199 DAB98046 7861F705
Certificate 2 is active.
 Issued by : C=  , ST= , L= , CN=10.6.41.138, O= , OU=
 Valid From: Apr 30 22:16:01 2003 GMT
 Valid to: Apr 29 22:16:01 2004 GMT
 Subject: C=  , ST= , L= , CN=10.6.41.138, O= , OU=
 SHA1 Fingerprint: 3DBDF89B 6B3E46A2 4255D023 42A361F2 90ED7042
```

802.1x Commands

aaa authentication dot1x

The **aaa authentication dot1x** Global Configuration mode command specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1x. Use the **no** form of this command to restore the default configuration.

Syntax

aaa authentication dot1x default *method1* [*method2*...]

no aaa authentication dot1x default

Parameters

- *method1* [*method2*...] — Specify at least one method from the following list:

Keyword	Description
RADIUS	Uses the list of all RADIUS servers for authentication
None	Uses no authentication

Default Configuration

No authentication method is defined.

Command Mode

Global Configuration mode

User Guidelines

Additional methods of authentication are used only if the previous method returns an error and not if the request for authentication is denied. To ensure that authentication succeeds even if all methods return an error, specify none as the final method in the command line.

The RADIUS server must support MD-5 challenge and EAP type frames.

Example

The following example uses the **aaa authentication dot1x default** command with no authentication.

```
Console# configure
Console(config)# aaa authentication dot1x default none
```

dot1x system-auth-control

The **dot1x system-auth-control** Global Configuration mode command enables 802.1x globally. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Default Configuration

802.1x is disabled globally.

Command Modes

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables 802.1x globally.

```
Console(config)# dot1x system-auth-control
```

dot1x port-control

The **dot1x port-control** Interface Configuration mode command enables manually controlling the authorization state of the port. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control

Parameters

- **auto** — Enables 802.1x authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the port and the client.
- **force-authorized** — Disables 802.1x authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1x-based authentication of the client.
- **force-unauthorized** — Denies all access through this interface by forcing the port to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through the interface.

Default Configuration

Port is in the force-authorized state

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in **auto** state that are connected to end stations), in order to get immediately to the forwarding state after successful authentication.

Example

The following example enables 802.1x authentication on Ethernet port e16.

```
Console(config)# interface ethernet e16
Console(config-if)# dot1x port-control auto
```

dot1x re-authentication

The **dot1x re-authentication** Interface Configuration mode command enables periodic re-authentication of the client. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x re-authentication

no dot1x re-authentication

Default Configuration

Periodic re-authentication is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables periodic re-authentication of the client.

```
Console(config)# interface ethernet e16
Console(config-if)# dot1x re-authentication
```

dot1x timeout re-authperiod

The **dot1x timeout re-authperiod** Interface Configuration mode command sets the number of seconds between re-authentication attempts. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

Parameters

- *seconds* — Number of seconds between re-authentication attempts. (Range: 300-4294967295)

Default Configuration

Re-authentication period is **3600** seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

There are no user guidelines for this command.

Example

The following example sets the number of seconds between re-authentication attempts, to 300.

```
Console(config)# interface ethernet e16
Console(config-if)# dot1x timeout re-authperiod 300
```

dot1x re-authenticate

The **dot1x re-authenticate** Privileged EXEC mode command manually initiates a re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.

Syntax

dot1x re-authenticate [**ethernet** *interface*]

Parameters

- *interface* — Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following command manually initiates a re-authentication of 802.1x-enabled Ethernet port e16.

```
Console# dot1x re-authenticate ethernet e16
```

dot1x timeout quiet-period

The **dot1x timeout quiet-period** Interface Configuration mode command sets the number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameters

- *seconds* — Specifies the time in seconds that the device remains in the quiet state following a failed authentication exchange with the client. (Range: 0-65535 seconds)

Default Configuration

Quiet period is **60** seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

During the quiet period, the device does not accept or initiate authentication requests.

The default value of this command should only be changed to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide a faster response time to the user, a smaller number than the default value should be entered.

Example

The following example sets the number of seconds that the device remains in the quiet state following a failed authentication exchange to 3600.

```
Console(config)# interface ethernet e16
Console(config-if)# dot1x timeout quiet-period 3600
```

dot1x timeout tx-period

The **dot1x timeout tx-period** Interface Configuration mode command sets the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Parameters

- *seconds* — Specifies the time in seconds that the device waits for a response to an EAP-request/identity frame from the client before resending the request. (Range: 30 - 65535 seconds)

Default Configuration

Timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following command sets the number of seconds that the device waits for a response to an EAP-request/identity frame, to 3600 seconds.

```
Console(config)# interface ethernet e16
Console(config-if)# dot1x timeout tx-period 3600
```

dot1x max-req

The **dot1x max-req** Interface Configuration mode command sets the maximum number of times that the device sends an Extensible Authentication Protocol (EAP)-request/identity frame (assuming that no response is received) to the client, before restarting the authentication process. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x max-req *count*

no dot1x max-req

Parameters

- *count* — Number of times that the device sends an EAP-request/identity frame before restarting the authentication process. (Range: 1-10)

Default Configuration

The default number of times is **2**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the number of times that the device sends an EAP-request/identity frame to 6.

```
Console(config)# interface ethernet e16
Console(config-if)# dot1x max-req 6
```

dot1x timeout supp-timeout

The **dot1x timeout supp-timeout** Interface Configuration mode command sets the time for the retransmission of an Extensible Authentication Protocol (EAP)-request frame to the client. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameters

- *seconds* — Time in seconds that the device waits for a response to an EAP-request frame from the client before resending the request. (Range: 1-65535 seconds)

Default Configuration

Default timeout period is **30** seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the timeout period before retransmitting an EAP-request frame to the client to 3600 seconds.

```
Console(config)# interface ethernet e16
Console(config-if)# dot1x timeout supp-timeout 3600
```

dot1x timeout server-timeout

The **dot1x timeout server-timeout** Interface Configuration mode command sets the time that the device waits for a response from the authentication server. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameters

- *seconds* — Time in seconds that the device waits for a response from the authentication server. (Range: 1-65535 seconds)

Default Configuration

The timeout period is **30** seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The actual timeout can be determined by comparing the **dot1x timeout server-timeout** value and the result of multiplying the **radius-server retransmit** value with the **radius-server timeout** value and selecting the lower of the two values.

Example

The following example sets the time for the retransmission of packets to the authentication server to 3600 seconds.

```
Console(config)# interface ethernet e16
Console(config-if)# dot1x timeout server-timeout 3600
```

show dot1x

The **show dot1x** Privileged EXEC mode command displays the 802.1x status of the device or specified interface.

Syntax

show dot1x [ethernet *interface***]**

Parameters

- *interface* — Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays the status of 802.1x-enabled Ethernet ports.

```
Console# show dot1x

802.1x is enabled

Port  Admin Mode  Oper Mode      Reauth  Reauth Username
                                 Control Period

----  ----------  ---------      ------- ------ --------
e1    Auto        Authorized     Ena     3600   Bob
e2    Auto        Authorized     Ena     3600   John
```

```
e3    Auto        Unauthorized   Ena     3600   Clark
e4    Force-auth  Authorized     Dis     3600   n/a
e5    Force-auth  Unauthorized*  Dis     3600   n/a

* Port is down or not present.


Console# show dot1x ethernet e3

802.1x is enabled.

Port  Admin Mode  Oper Mode      Reauth  Reauth  Username
                                 Control Period
----  ----------  ---------      ------- ------  --------
e3    Auto        Unauthorized   Ena     3600    Clark


Quiet period:60 Seconds
Tx period:30 Seconds
Max req: 2
Supplicant timeout: 30 Seconds
Server timeout: 30 Seconds
Session Time (HH:MM:SS): 08:19:17
MAC Address: 00:08:78:32:98:78
Authentication Method: Remote
Termination Cause: Supplicant logoff


Authenticator State Machine
State: HELD


Backend State Machine
State: IDLE
Authentication success: 9
Authentication fails: 1
```

The following table describes the significant fields shown in the display.

Field	Description
Port	The port number.
Admin mode	The port admin mode. Possible values: Force-auth, Force-unauth, Auto.
Oper mode	The port oper mode. Possible values: Authorized, Unauthorized or Down.
Reauth Control	Reauthentication control.
Reauth Period	Reauthentication period.
Username	The username representing the identity of the Supplicant. This field shows the username in case the port control is auto. If the port is Authorized, it shows the username of the current user. If the port is unauthorized it shows the last user authenticated successfully.
Quiet period	The number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
Tx period	The number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before resending the request.
Max req	The maximum number of times that the device sends an Extensible Authentication Protocol (EAP)-request frame (assuming that no response is received) to the client before restarting the authentication process.
Supplicant timeout	Time in seconds the switch waits for a response to an EAP-request frame from the client before resending the request.
Server timeout	Time in seconds the switch waits for a response from the authentication server before resending the request.
Session Time	The amount of time the user is logged in.
MAC address	The supplicant MAC address.
Authentication Method	The authentication method used to establish the session.

Field	Description
Termination Cause	The reason for the session termination.
State	The current value of the Authenticator PAE state machine and of the Backend state machine.
Authentication success	The number of times the state machine received a Success message from the Authentication Server.
Authentication fails	The number of times the state machine received a Failure message from the Authentication Server.

show dot1x users

The **show dot1x users** Privileged EXEC mode command displays active 802.1x authenticated users for the device.

Syntax

show dot1x users [username *username*]

Parameters

- *username* — Supplicant username (Range: 1-160 characters)

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays 802.1x users.

```
console(config-if)# show dot1x users

                           Session     Auth     MAC
Port    Username     Time        Method   Address            VLAN
------ ----------- ---------- ------   --------------     ----
e1      dva5         00:00:06    Remote   00:05:74:94:2a:1c  5
e2      admin        00:04:04    Remote   00:05:1c:18:0a:7e
```

The following table describes the significant fields shown in the display.

Field	Description
Port	The port number.
Username	The username representing the identity of the Supplicant. This field shows the username in case the port control is auto. If the port is Authorized, it shows the username of the current user. If the port is unauthorized it shows the last user authenticated successfully.
Session Time	The amount of time the user is logged in.
MAC address	The supplicant MAC address.
Authentication Method	The authentication method used to establish the session.

show dot1x statistics

The **show dot1x statistics** Privileged EXEC mode command displays 802.1x statistics for the specified interface.

Syntax

show dot1x statistics ethernet *interface*

Parameters

- *interface* — Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays 802.1x statistics for the specified interface.

```
Console# show dot1x statistics ethernet e1

EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 12
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:08:78:32:98:78
```

The following table describes the significant fields shown in the display:

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	The number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
EapolReqIdFramesTx	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

Advanced Features

dot1x auth-not-req

The **dot1x auth-not-req** Interface Configuration (VLAN) mode command enables unauthorized devices access to the VLAN. Use the **no** form of this command to disable access to the VLAN.

Syntax

dot1x auth-not-req

no dot1x auth-not-req

Default Configuration

Access is enabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

An access port cannot be a member in an unauthenticated VLAN.

The native VLAN of a trunk port cannot be an unauthenticated VLAN.

For a general port, the PVID can be an unauthenticated VLAN (although only tagged packets are accepted in the unauthorized state.)

Example

The following example enables access to the VLAN to unauthorized devices.

```
Console(config)# interface vlan 5
Console(config-if)# dot1x auth-not-req
```

dot1x multiple-hosts

The **dot1x multiple-hosts** Interface Configuration mode command enables multiple hosts (clients) on an 802.1x-authorized port, where the authorization state of the port is set to auto. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x multiple-hosts [**authentication**]

no dot1x multiple-hosts

Parameters

- **authentication** — Specifies that each station should be 802.1x authenticated. This mode is also called ‘multiple sessions’.

Default Configuration

Multiple hosts are disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

This command enables attaching multiple clients to a single 802.1X-enabled port.

If this command is used without the authentication keyword, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.

If this command is used with the authentication keyword, each host must be successfully authorized in order to grant network access. Please note that packets are NOT encrypted, and after successful authentication, filtering is based on the source MAC address only.

For unauthenticated VLANs, multiple hosts are always enabled.

Port security cannot be enabled on a port if multiple hosts mode is disabled, or if multiple hosts with authentication per host mode is enabled.

It is recommended to enable reauthentication when working in ‘multiple sessions (multiple-hosts authentication)’, in order to detect ‘user logout’ for users who have not yet sent ‘logoff’.

Example

The following command enables multiple hosts (clients) on an 802.1x-authorized port.

```
Console(config)# interface ethernet e16
Console(config-if)# dot1x multiple-hosts
```

dot1x radius-attributes vlan

Use the **dot1x radius-attributes vlan** interface configuration command, to enable user-based VLAN assignment. Use the **no** form of this command to disable user-based VLAN assignment.

Syntax

dot1x radius-attributes vlan

no dot1x radius-attributes vlan

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled.

Command Mode

Interface configuration (Ethernet)

User Guidelines

- User-based VLAN assignment is supported only in 802.1x multiple sessions.
- The configuration of the parameter is allowed only when the port is Forced Authorized or Forced Unauthorized.

dot1x single-host-violation

The **dot1x single-host-violation** Interface Configuration (Ethernet) mode command configures the action to be taken when a station whose MAC address is not the supplicant MAC address attempts to access the interface. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x single-host-violation {**forward** | **discard** | **discard-shutdown**} [**trap** *seconds*]

o dot1x single-host-violation

Parameters

- **forward —** Specifies that each station should be 802.1x authenticated. This mode is also called 'multiple sessions'.
- **discard —** Discards frames with source addresses that are not the supplicant address.
- **discard-shutdown —** Discards frames with source addresses that are not the supplicant address. The port is also shut down.
- **trap** *seconds*—Indicates that SNMP traps are sent. Specifies the minimum amount of time in seconds between consecutive traps. (Range: 1- 1000000)

Default Configuration

Frames with source addresses that are not the supplicant address are discarded. No Traps.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The command is relevant when Multiple hosts is disabled and the user has been successfully authenticated.

A BPDU message with a MAC address that is not the supplicant MAC address is not discarded in discard mode.

A BPDU message with a MAC address that is not the supplicant MAC address causes a shutdown in discard-shutdown mode for GE ports, and is not discarded for FE ports.

Example

The following command shuts down port e5 upon an unsuccessful authentication attempt on the port

```
Console(config)# interface ethernet 5
Console(config-if)# dot1x single-host-violation discard-
shutdown
```

dot1x bpdu

Use the dot1x bpdu global configuration command to define 802.1x BPDU handling when 802.1x is globally disabled. Use the no form of this command to return to default.

Syntax

dot1x bpdu {filtering | bridging}

no dot1x bpdu

Parameters

- **filtering** — Specify that when 802.1x is globally disabled, 802.1x BPDU packets would be filtered.
- **bridging** — Specify that when 802.1x is globally disabled, 802.1x BPDU packets would be bridged.

Default

The default value is **filtering**.

Command Modes

Global configuration

Usage Guidelines

According to IEEE802.1 standards the 802.1X BPDUs should never be forwarded. The 802.1X BPDUs should be handled by the software in case 802.1X is enabled on the ingress port, or discarded in all other cases.

This feature enables to bridge 802.1X BPDUs packets as data packets.

The feature can be enabled only when 802.1X is globally disabled (by the no dot1x system-auth-control global configuration command). If the port is disabled for 802.1X but 802.1X is enabled globally, 802.1X BPDUs would always be discarded.

Examples

```
Console(config)# dot1x bpdu bridging
```

show dot1x bpdu

Use the **show dot1x bpdu** EXEC command to display the 802.1x BPDU handling when 802.1x is globally disabled.

Syntax

show dot1x bpdu

Parameters

This command has no arguments or keywords.

Default Configuration

This command has no default configuration.

Command Modes

EXEC

User Guidelines

There are no user guidelines for this command.

Examples

```
Switch# show dot1x bpdu

802.1X BPDU packets are trapped for the 802.1X protocol.


Switch# show dot1x bpdu

802.1X BPDU packets are filtered.
```

```
Switch# show dot1x bpdu

802.1X BPDU packets are bridged.
```

dot1x guest-vlan

The **dot1x guest-vlan** Interface Configuration (VLAN) mode command defines a guest VLAN. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x guest-vlan

no dot1x guest-vlan

Default Configuration

No VLAN is defined as a guest VLAN.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Use the **dot1x guest-vlan enable** Interface Configuration mode command to enable unauthorized users on an interface to access the guest VLAN.

If the guest VLAN is defined and enabled, the port automatically joins the guest VLAN when the port is unauthorized and leaves it when the port becomes authorized. To be able to join or leave the guest VLAN, the port should not be a static member of the guest VLAN.

Example

The following example defines VLAN 2 as a guest VLAN.

```
Console# configure
Console(config)# vlan database
Console(config-vlan)# vlan 2
Console(config-vlan)# exit
Console(config)# nterface vlan 2
Console(config-if)# dot1x guest-vlan
```

dot1x guest-vlan enable

The **dot1x vlans guest-vlan enable** Interface Configuration mode command enables unauthorized users on the interface access to the Guest VLAN. Use the **no** form of this command to disable access.

Syntax

dot1x guest-vlan enable

no dot1x guest-vlan enable

Default Configuration

Disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

A device can have only one global guest VLAN. The guest VLAN is defined using the **dot1x guest-vlan** Interface Configuration mode command.

Example

The following example enables unauthorized users on Ethernet port e1 to access the guest VLAN.

```
Console# configure
Console(config)# interface ethernet e1
Console(config-if)# dot1x guest-vlan enable
```

dot1x mac-authentication

The **mac-authentication** Interface Configuration mode command enables authentication based on the station's MAC address. Use the **no** form of this command to disable MAC authentication.

Syntax

dot1x mac-authentication {**mac-only** | **mac-and-802.1x**}

no dot1x mac-authentication

Parameters

- **mac-only —** Enable authentication based on the station's MAC address only. 802.1X frames are ignored.
- **mac-and-802.1x —**Enable 802.1X authentication and MAC address authentication on the interface.

Default Configuration

The default configuration is **disabled**.

Command Mode

Interface configuration (Ethernet)

User Guidelines

Guest VLAN must be enabled, when MAC authentication is enabled.

Static MAC addresses can't be authorized. Do not change authenticated MAC address to static address.

It is not recommended to delete authenticated MAC addresses. Reauthentication must be enabled when working in this mode.

When the device sends a MAC address as the 802.1x user name or password to a RADIUS server, the characters ":" and "-" are not forwarded to the Radius server. Avoid defining the corresponding MAC address with ":" and "-" in the RADIUS server.

Example

The following example enable authentication based on the station's MAC address. Use the **no** form of this command to disable MAC authentication.

```
Console# configure
Console(config)# interface ethernet e1
Console(config-if)# dot1x mac-authentication
```

show dot1x advanced

The **show dot1x advanced** Privileged EXEC mode command displays 802.1x advanced features for the device or specified interface.

Syntax

show dot1x advanced [**ethernet** *interface*]

Parameters

- *interface* — Valid Ethernet port.

Default Configuration

This command has no default configuration.

Command Mode

Privileged EXEC mode

User Guidelines

There are no user guidelines for this command.

Example

The following example displays 802.1x advanced features for the device.

```
Console# show dot1x advanced

Guest VLAN: 3978

Unauthenticated VLANs: 91,92

Interface  Multiple   Guest         MAC             VLAN
           Hosts      VLAN          Authentication  Assignment
---------  ---------  ------------  --------------  ----------
e1         Disabled   Enabled       MAC-and-802.1X  Enabled
e2         Enabled    Enabled       MAC-and-802.1X  Enabled


Console# show dot1x advanced ethernet e1

Guest VLAN: 2

Unauthenticated VLANs: 91,92

Interface  Guest VLANS
---------  -----------
e1         Enabled

Trap: Enabled
Trap frequency: 100
```

A

Alias Names

Alias Name Support

The table below defines alias names and their corresponding "native" command names, as supported on the switch. Input parameter variations and/or returned responses for commands launched with alias names are defined in the native command's description in this guide.

NOTE Alias names are supported by the SPS208G, SPS224G4, and SPS2024 switches.

Native Command	Alias Command
copy running-config startup-config	write (wr)
configure	configure terminal
show bridge address-table	show mac address-table
show interfaces configuration interface	show interfaces
show ip dhcp information option	show ip dhcp snooping information option
show ip source-guard configuration	show ip verify source

B

Where to Go From Here

Product Resources

Website addresses in this document are listed without **http://** in front of the address because most current web browsers do not require it. If you use an older web browser, you may have to add **http://** in front of the web address.

Resource	Link
Cisco Partner Central (requires partner registration and login)	www.cisco.com/web/partners/sell/smb/
Cisco Small Medium Business Product Information	www.cisco.com/go/smallbiz

Related Documentation

For additional information about the Ethernet switches, see the *SPS208G/SPS224G4/SPS2024 Ethernet Switches Administration Guide.*

C

Additional Information

Regulatory Compliance and Safety Information

Regulatory Compliance and Safety Information for this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz

Warranty

Warranty information that applies to this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz

End User License Agreement (EULA)

Licensing information that applies to this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz

D

Support Contacts

Support contact information for this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz